Systems Engineering Philosophies and Principles at JPL

Thomas Randolph

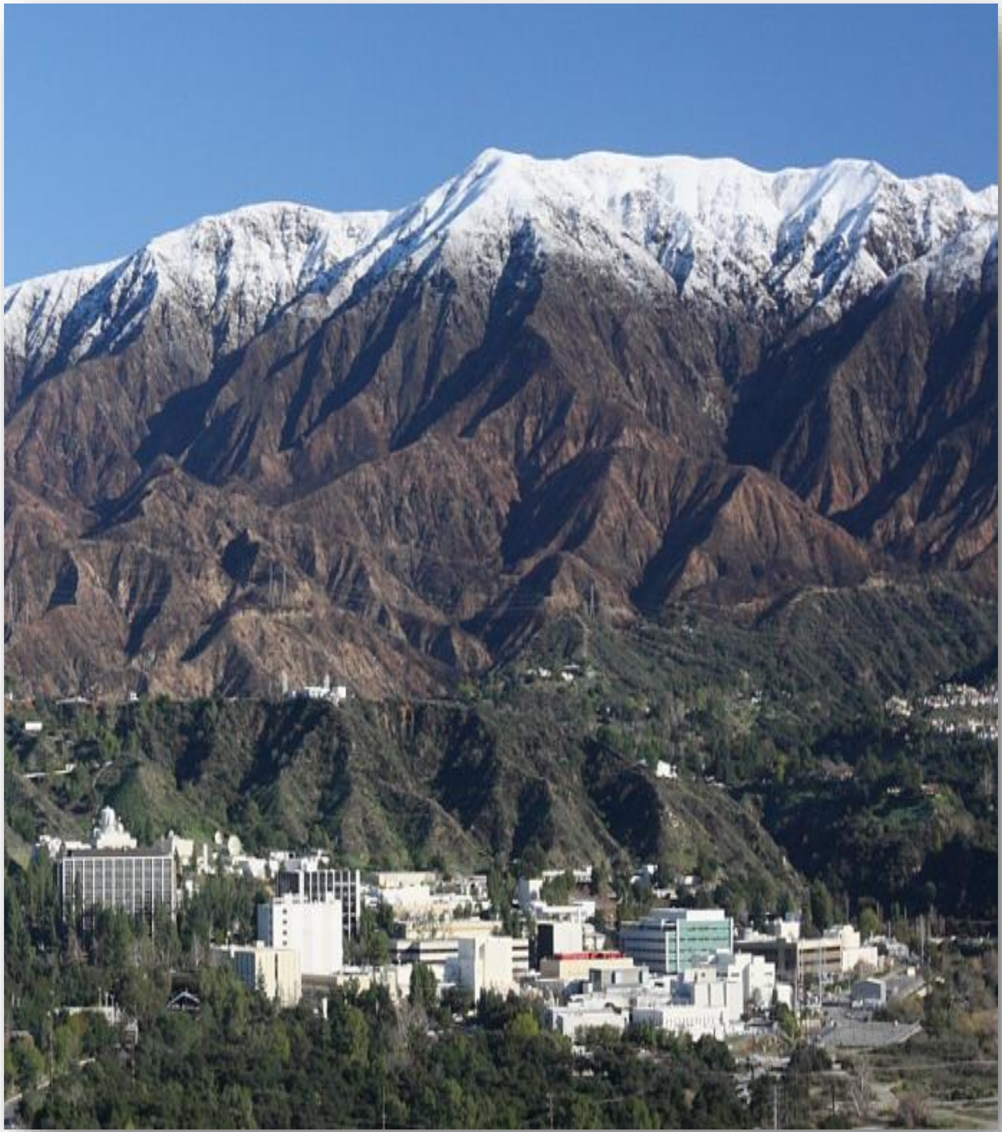
Project Manager, Principal Engineer
Project Systems Engineering and Formulation Section
Jet Propulsion Laboratory, California Institute of Technology

February 9, 2018
Tsukuba Space Center, Japan

JPL is Part of NASA and Caltech

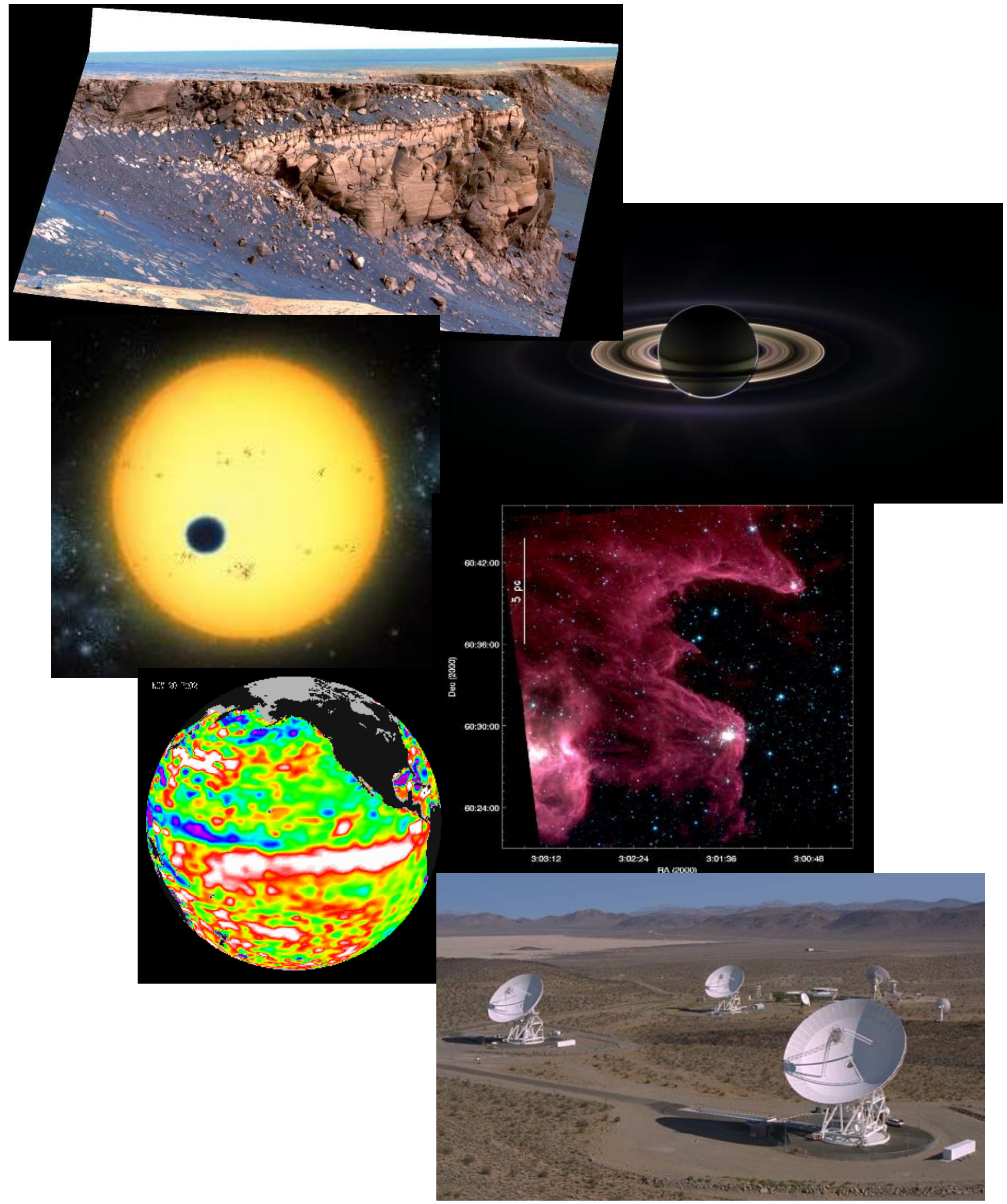
Jet Propulsion Laboratory
California Institute of Technology

- A NASA Center
- Federally-funded (NASA-owned) Research and Development Center (FFRDC)
- University Operated (Caltech)
- $1.8B Business Base
- 6,000 Employees



JPL's Mission for NASA is *Robotic* Space Exploration

- **Mars**
- **Solar system**
- **Exoplanets**
- **Astrophysics**
- **Earth Science**
- **Interplanetary network**



JPL Through the Years

Jet Propulsion Laboratory
California Institute of Technology

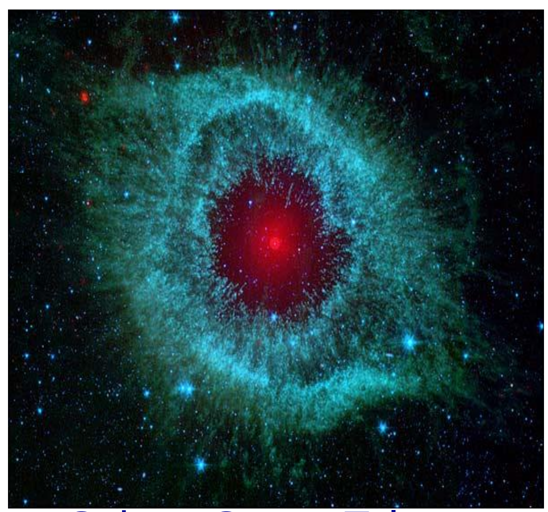
From Caltech students testing rockets to exploring the planets

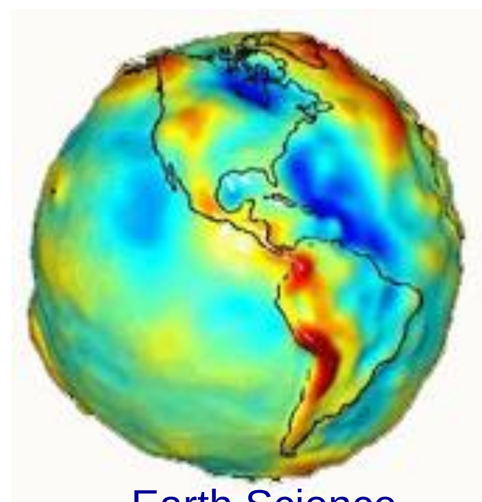

Caltech students (1936)


Missiles (1940s)


Explorer 1 (1958)


Mars Exploration Rovers (2004 – present)


Spitzer Space Telescope (2004 – present)


Earth Science (1978 – now)

The Beginning of Systems Engineering at JPL

- **The rocket era was the incubator for the Systems Approach**
  - Recognition that rockets were not being designed as "systems"
    - Organization traced to academic disciplines
    - Could achieve only 60% reliability, even with hand-holding
  - William Pickering: *"right from the very beginning there must be a clear concept of of what the...system is supposed to do. The system should be ready for production, completely documented, properly designed, consistent with all requirements; training programs ready to go…manuals written and supply channels activated…"*
  - *The systems approach meant including reliability, testing, and maintenance considerations early in the design process. Systems engineering incorporated those activities that ensure coordination among the various design activities.*
- **By applying a systems engineering discipline, JPL developed the procedural expertise necessary to convert research technology in operational systems.**
- **This culminated in the successful launch and operations of the Explorer 1 satellite.**

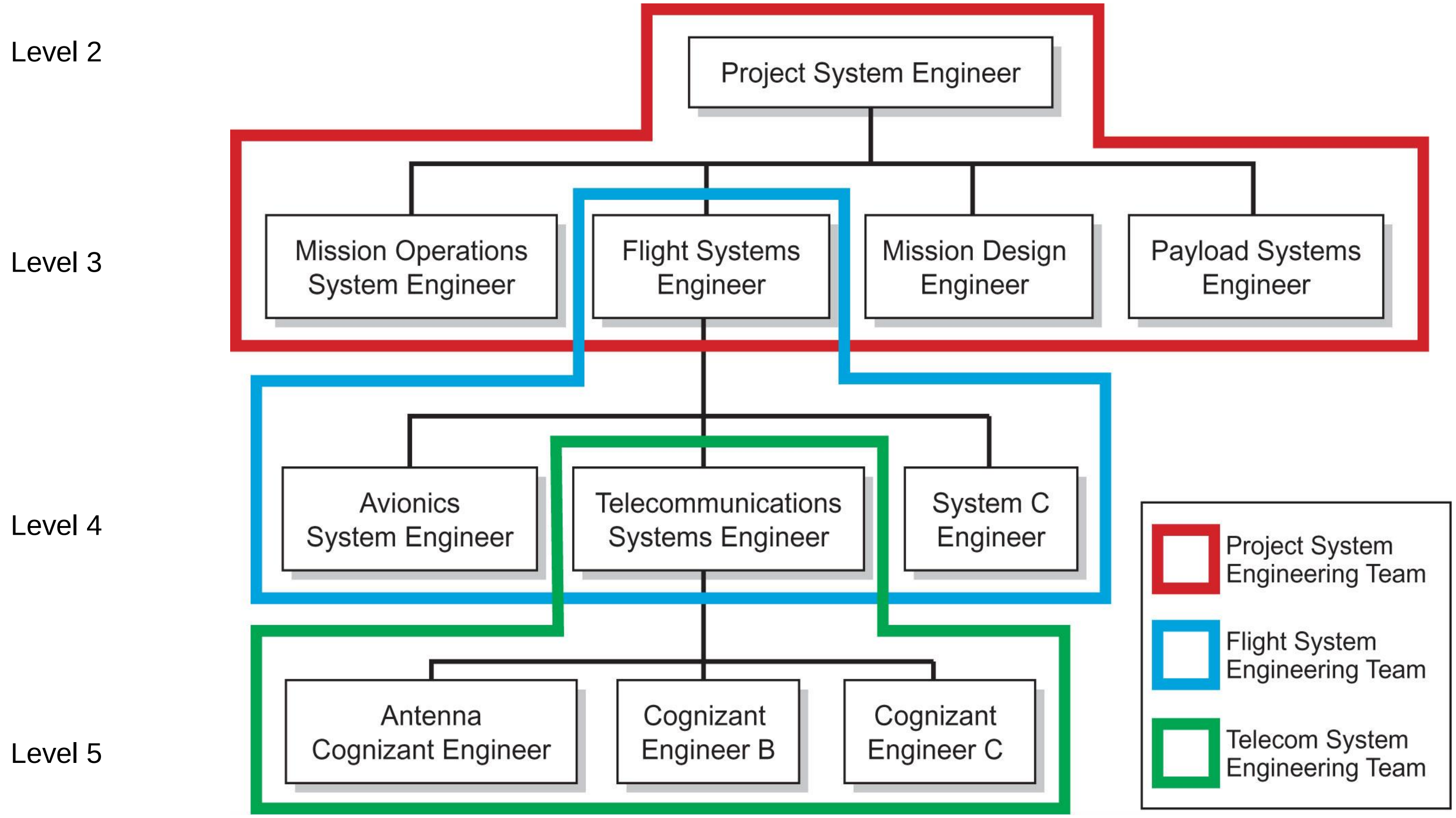
On to Spacecraft-Ranger and Mariner

- **Ranger (Lunar photos prior to impact)**
  - PM chose to maintain the launch schedule regardless of technical difficulties
  - PM did not have any Systems Engineering partner
  - Poor communications with the LV supplier, little oversight
  - Rapid growth at JPL stretched the availability of senior engineers
  - Rangers 1-6 ended in failure

- **Mariner (scientific Venus and Mars fly-bys)**
  - PM came from Systems Engineering
  - Established rigorous SE processes
    - Development of specifications and design was tracked, not just hardware
    - Instituted progressive design freezes with strong configuration control (ECRs)
    - Instituted Problem reporting
    - Extended the concept of hardware interface definition to operational and management interfaces.
    - Created the Project Policy and Requirements Document
    - Led to the establishment of the "Spacecraft Systems Engineer"
    - The Mariner program is considered a great success

System, not Craft

System Engineering at JPL



PSE Role Statement

The Project Systems Engineer (PSE) is responsible for project technical integrity including mission risk and performance to meet the driving scientific and technological objectives. The PSE is responsible for the planning and implementation of the system engineering function <u>across the entire scope of the project</u>.

The JPL Systems Engineering Practices are organized according to ten systems engineering functions:

Function **Examples**

1. Architecting: "**Describe the architecture using different views**"

2. Requirements: "**Trace reqs to a parent if not locally-derived**"

3. Analyzing and Characterizing the Design: "**Validate models used to specify elements**"

4. Managing Technical Resources and Performance: "**Identify & manage key technical resources**"

5. Interfaces: "**Use common units and determine controls**"

6. Verification and Validation: "**Ensure verification of all requirements**"

7. Reviews: "**Ensure completion of AIs from reviews**"

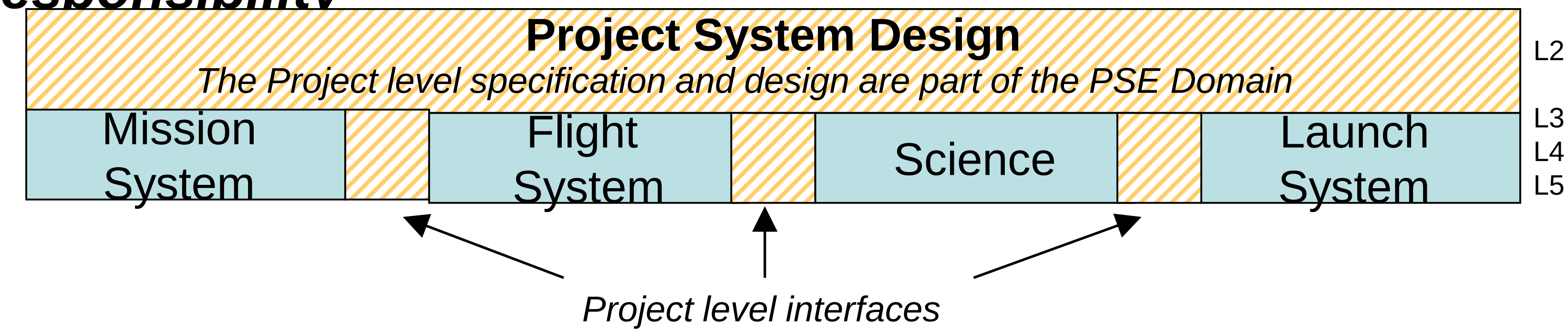
8. Risk Management: "**Ensure risk mitigations are verified**"

9. Managing & Controlling the Design: "**Manage assessments of proposed changes**"

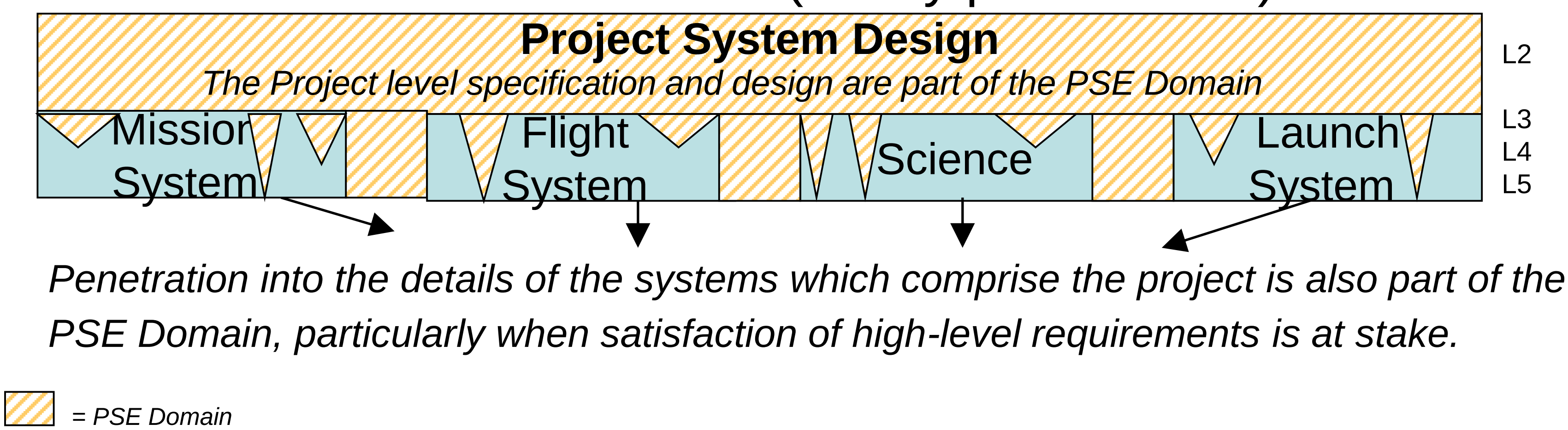
10. Managing the Systems Engineering Task: "**Update the SE plan prior to the next phase**"

What is the PSE's Scope?

- The first diagram shows PSE Domain = ***PSE delivery responsibility***

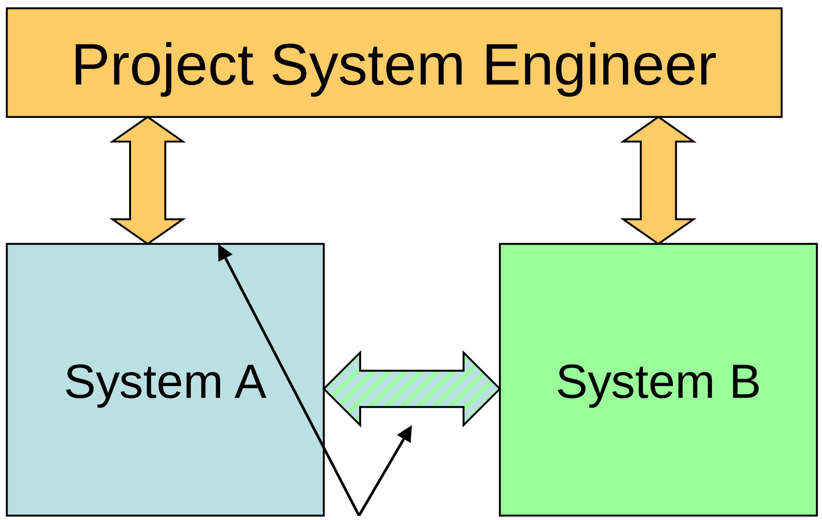


- But, as is the case with all systems engineers, in reality the boundaries are not so clear-cut when it comes to ***influencing*** the overall design. The second diagram more accurately shows how the PSE works in terms of ***influence*** (at any point in time)



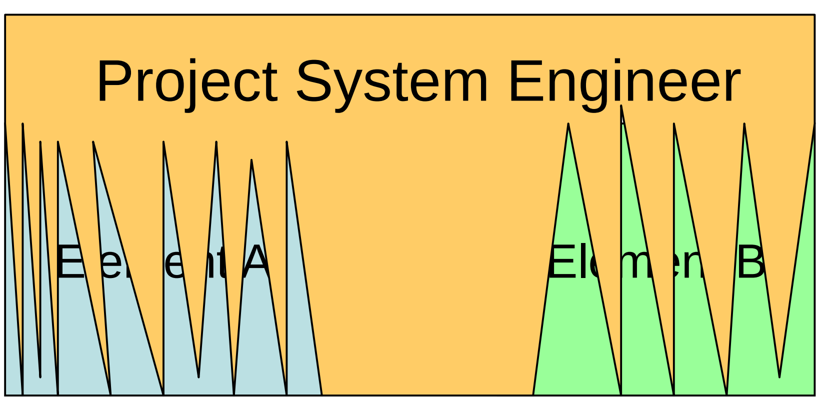
When & How to "Go Deep" *(the Jello-Cake Model)*

NOT THIS!



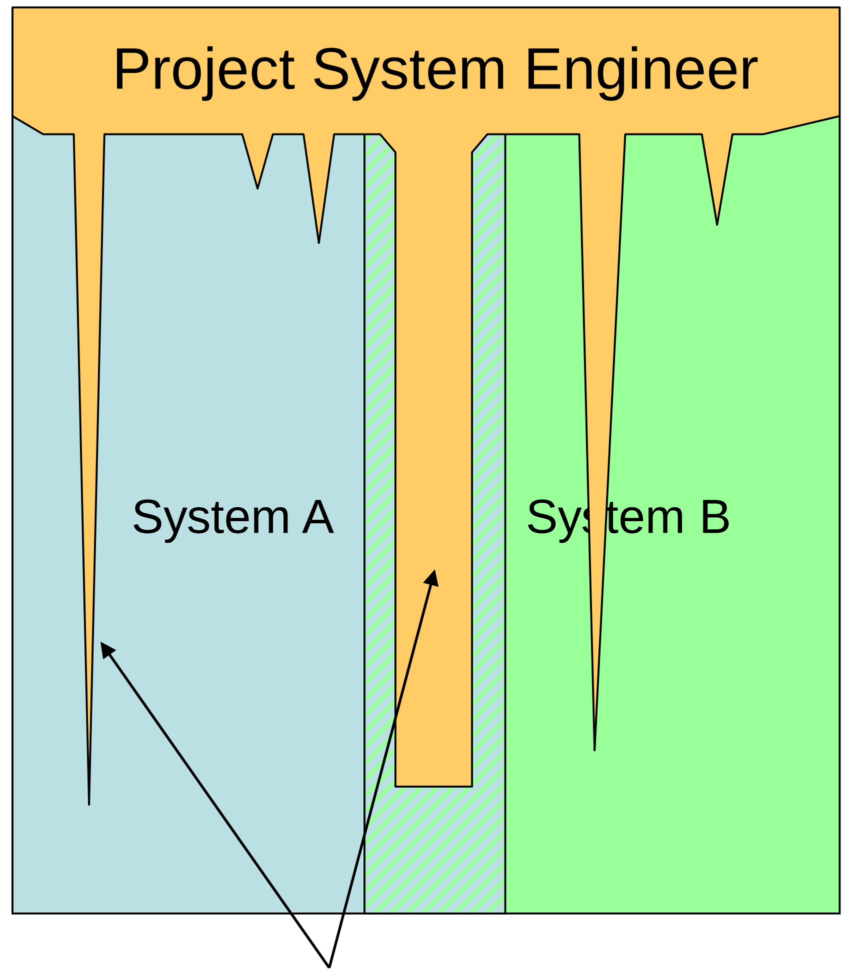
Don't want firewalls and Rec/Del driven approach

NOR THIS!!



Let things bubble up – nobody's omniscient

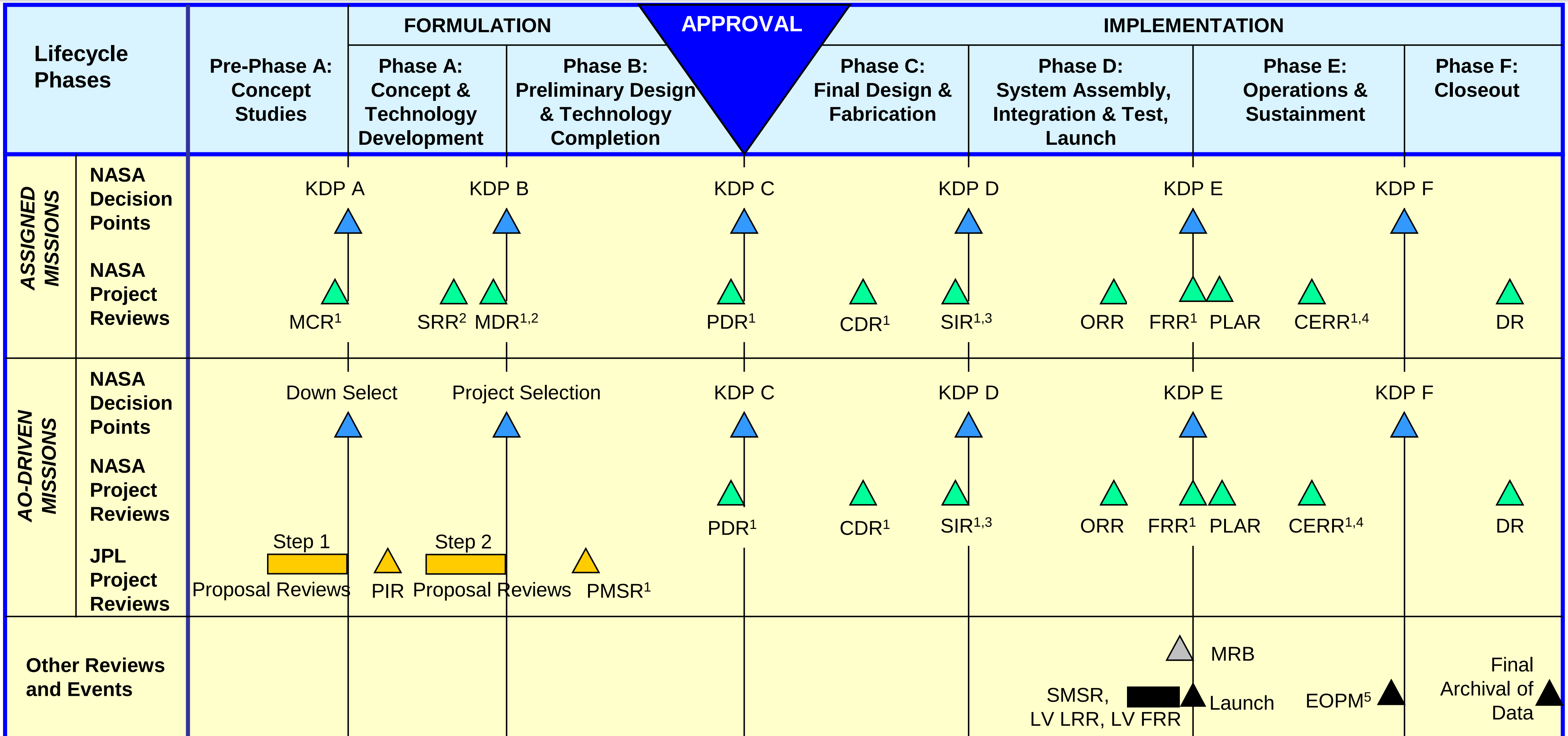
WANT <u>THIS</u>



PSE lives at Level 2 & interface between 2+1 elements *and* selectively goes deep to penetrate vacuums & FACILATE their resolution. (Get the right people engaged to solve the problem. These are often people working across the interfaces that you control.)

National Aeronautics and Space Administration
Jet Propulsion Laboratory
California Institute of Technology

The NASA/JPL Project Lifecycle



Notes

(1) Review is followed by a JPL CMC. If the review immediately precedes a KDP, a Mission Directorate and/or Agency PMC/GPMC, as appropriate, are required prior to the KDP.
(2) The SRR and MDR may be combined
(3) SIR is a “soft gate”, project may initiate Phase D work immediately upon completion of Phase C work products, absent a notice of discontinuance from the Program Manager
(4) CERRs are established at the discretion of Program Offices.
(5) At the end of the prime mission, if an extended mission is approved, the extended mission is still in Phase E.

Legend

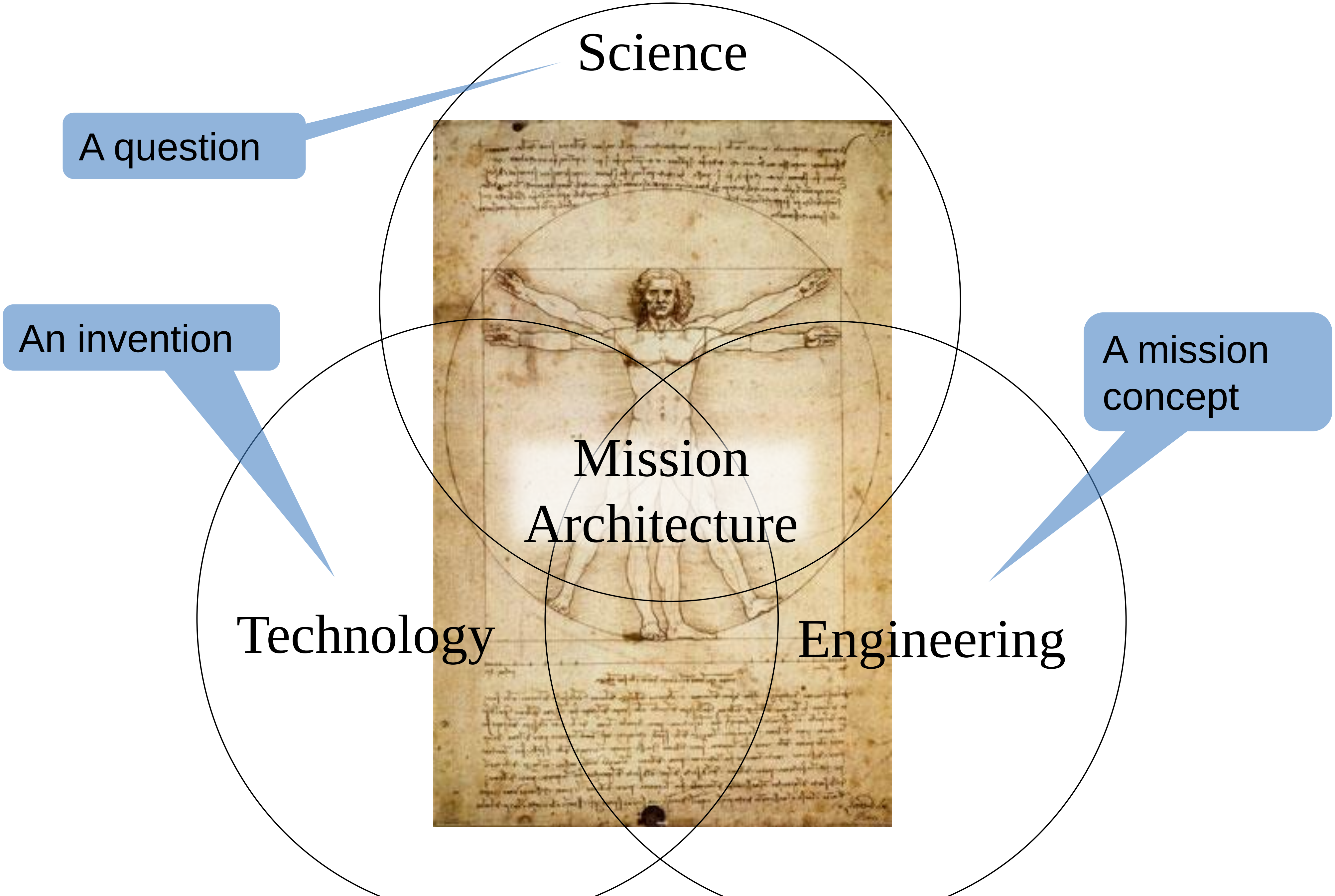
CDR – Critical Design Review
CERR – Critical Events Readiness Review
CMC – Center Management Council
DR – Decommissioning Review
EOPM – End of Prime Mission
FRR – Flight Readiness Review
GPMC – Governing Program Management Council
KDP – Key Decision Point
LV FRR – Launch Vehicle Flight Readiness Review
LV LRR – Launch Vehicle Launch Readiness Review
MCR – Mission Concept Review
MDR – Mission Definition Review
MRB – Mission Readiness Briefing
ORR – Operations Readiness Review
PDR – Preliminary Design Review
PIR – Proposal Implementation Review
PLAR – Post Launch Assessment Review
PMC – Program Management Council
PMSR – Project Mission System Review
SIR – System Integration Review
SMSR – Safety and Mission Success Review
SRR – System Requirements Review

05.01.2007

JPL's Innovation Foundry

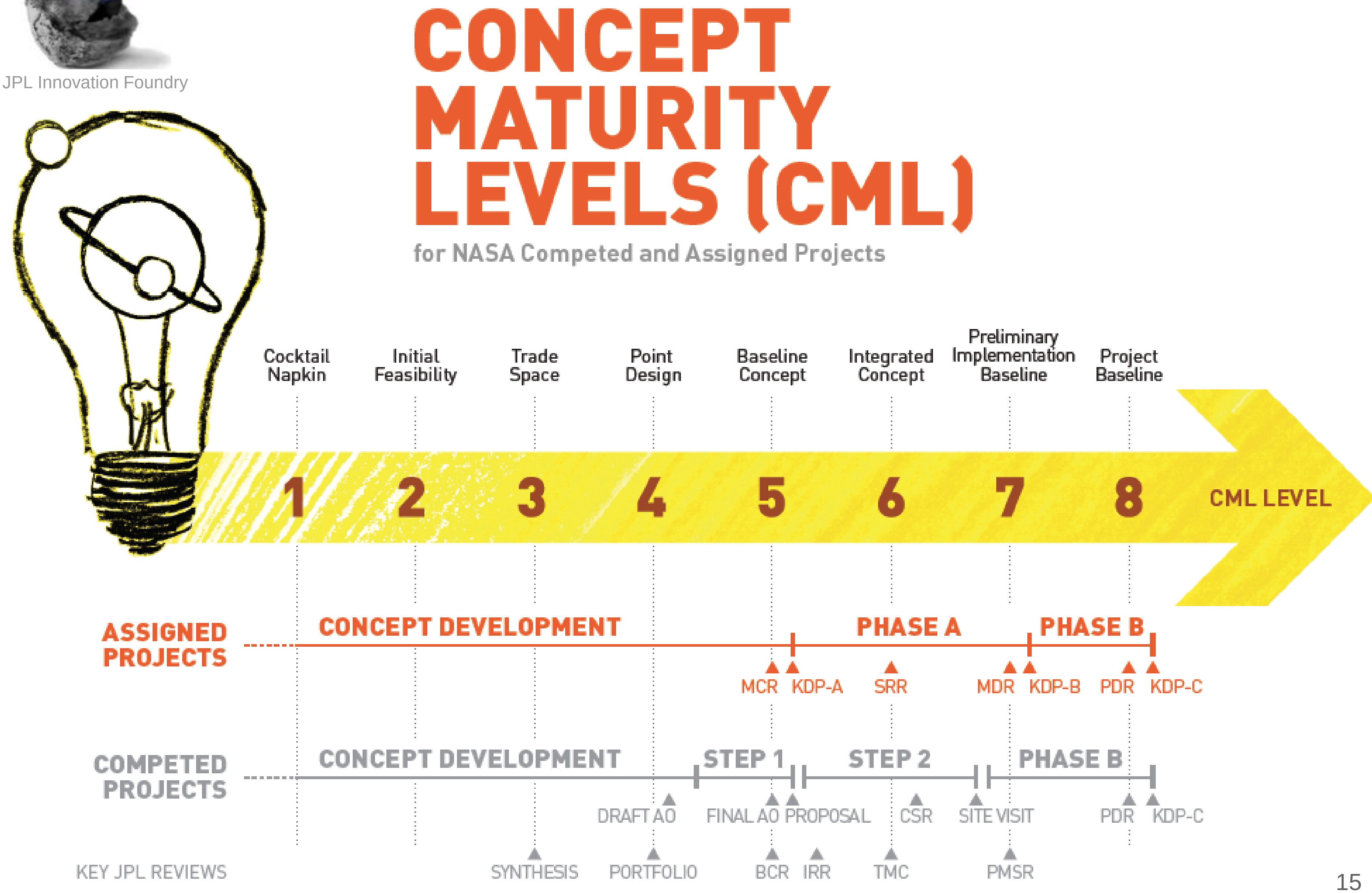
- **JPL supports the science community to ideate, mature, and propose concepts for new NASA missions**
- **JPL continuously "system engineers" requirements and solutions to develop compelling new missions**
- **The JPL Innovation Foundry is our integrated formulation lifecycle enterprise**

Every Mission Starts with a Spark

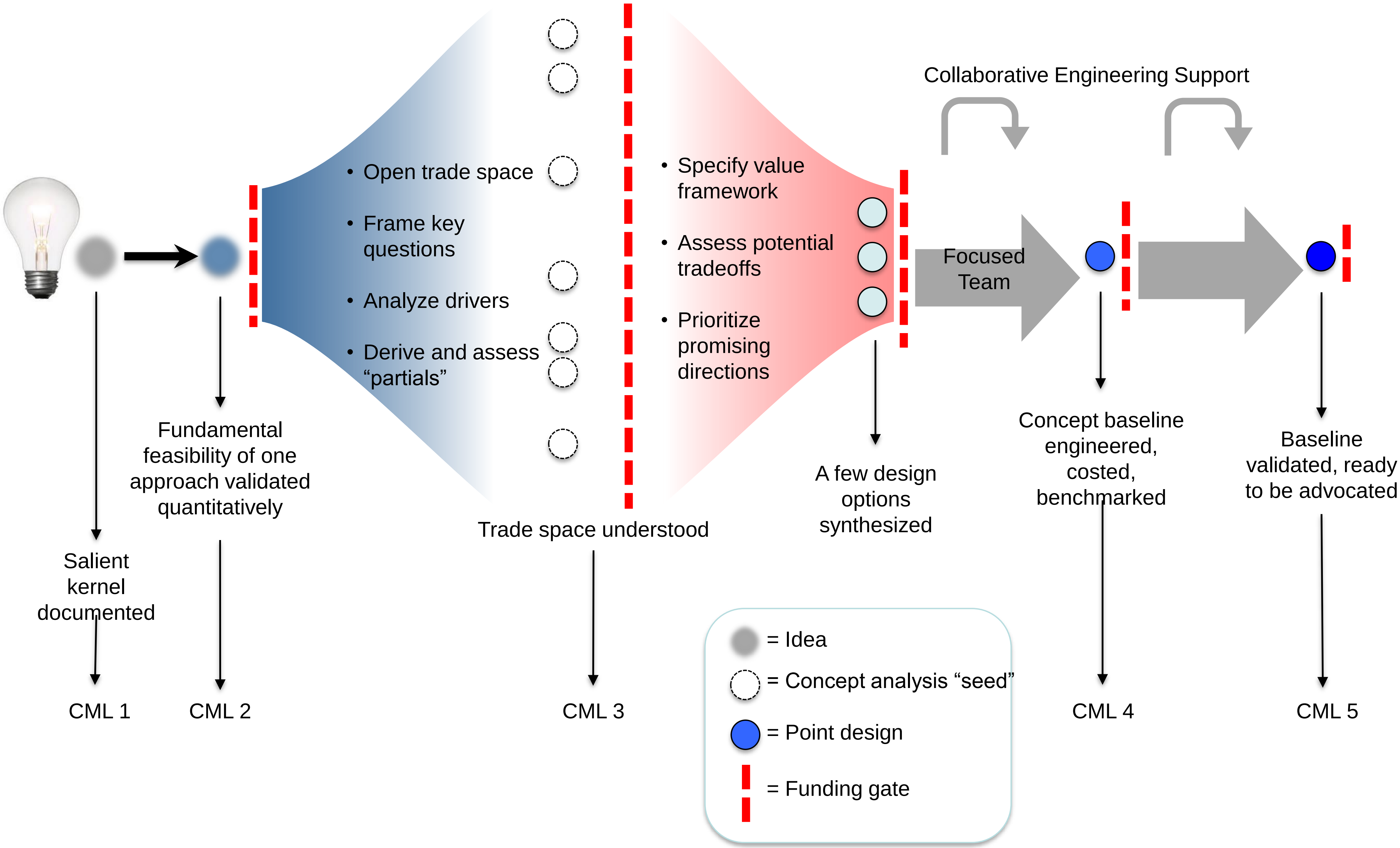


CMLs Correspond to Life Cycle Milestones

JPL Innovation Foundry



Evolution of an Idea



The A-Team

The A-Team efficiently explores the science, implementation, and programmatic trade space in early concept formulation.

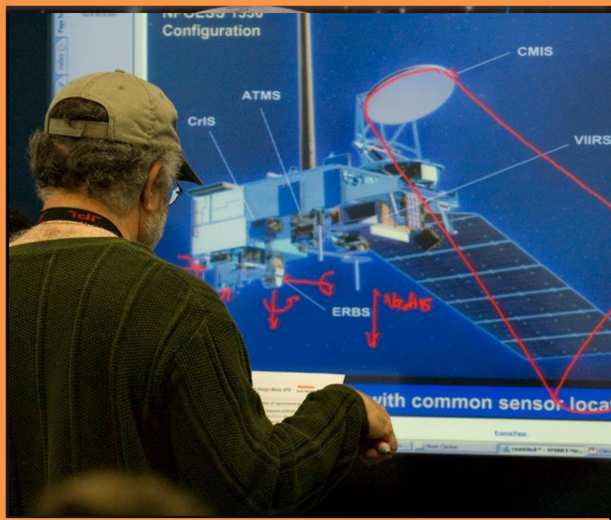
The A-Team Study Types

CML 1: Idea Generation	• Produce 100's of ideas from a single question or topic • Organize and potentially rank ideas based on figures of merit
CML 2: Feasibility Assessment	• Quantitatively examine an idea or set of ideas for both technical and programmatic feasibility using advanced analysis tools
CML 3: Trade Space Exploration	• Efficiently explore the value, cost, and risk trade space for concepts and new processes
Science	• Develop the science story and investigation - link goals, objectives, measurements, and instruments including assessing relative science value
Technology	• Generate list of potential applications and assess feasibility and benefit • Quantitatively examine the science mission and architecture impacts
Architecture	• Design "prototype" concepts based on science "seeds" • Rapidly analyze options with multiple design iterations to find key drivers
Strategy	• Investigate the programmatic aspects including portfolio building, strategic directions, decision support, and proposal strategy


active
corpus

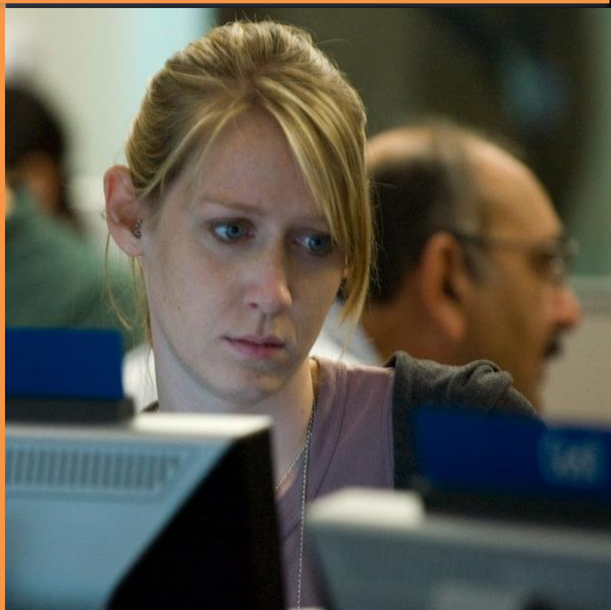

Concept for an outerplanet Probe
mass= 940KG


TEAM X
Jet Propulsion Laboratory


Configuration
CMIS
ATMS
CrIS
VIIRS
ERBS


TEAM X

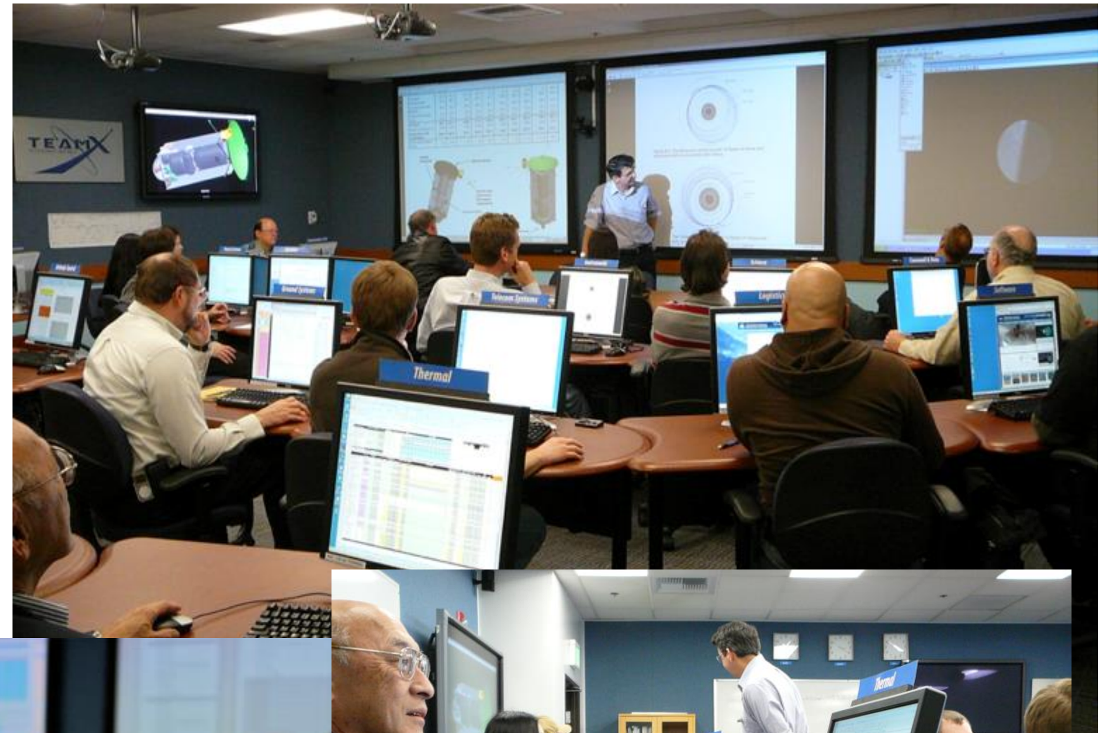

N
Team X Operations Manager
Storage
Instrument Study Team Area C
CUSTOMER
Storage
Architecture Study Team Area B
Storage
CUSTOMER
Mission Study Team Area A
System Administrators
Storage



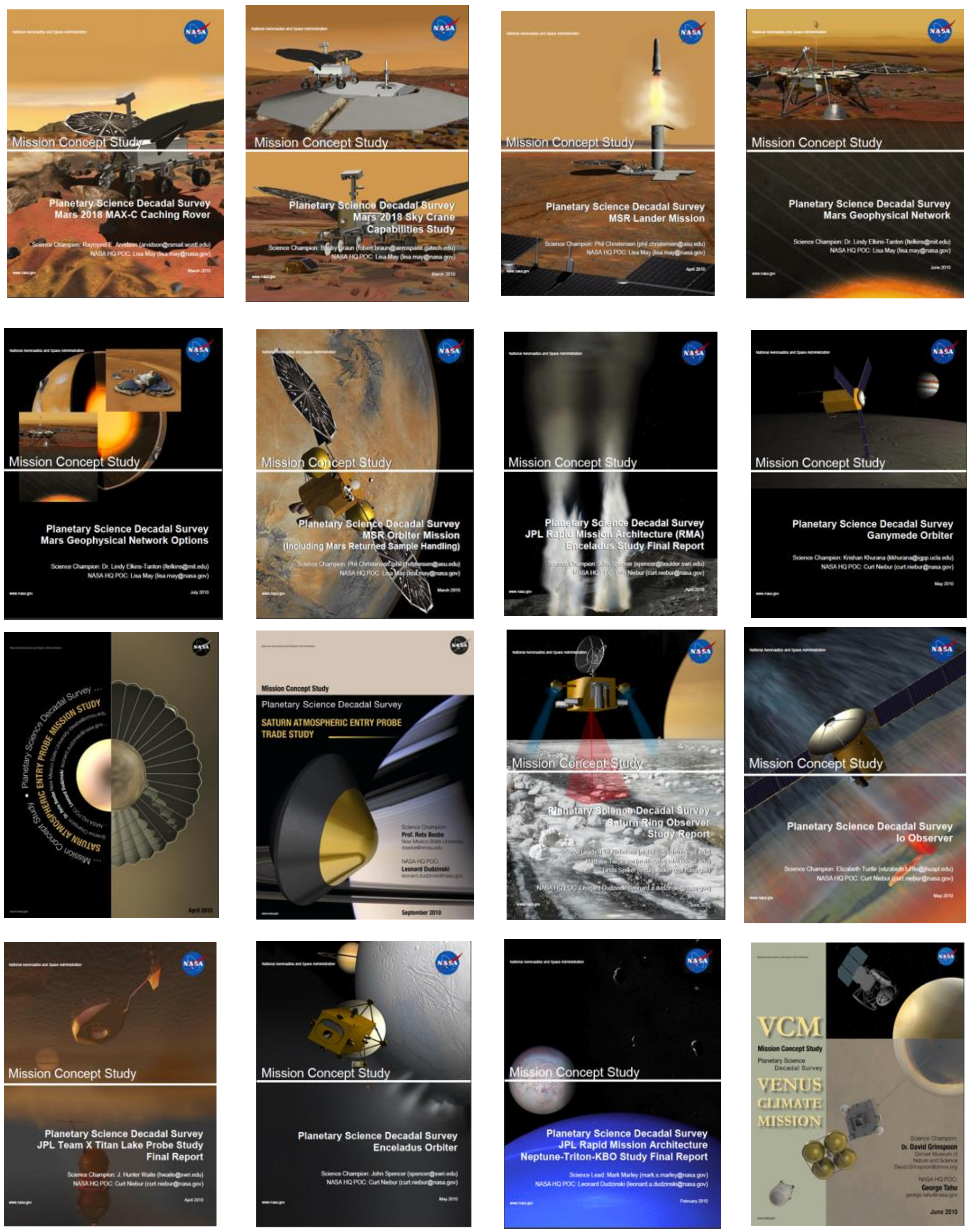
10^3 Team X Studies

Team X is a concurrent engineering team for rapid design and analysis of novel space mission concepts

- Backed by refined and validated, institutionally supported, integrated tools, models, and processes
- Staffed and backed by doing organizations
- Well-suited for all aspects of Pre-Phase A and Phase A design activities



High Visibility Products for NASA



- **Team X supported 16 mission concepts for Planetary Science Decadal Survey**
- **Team X supported 14 instrument and mission concepts for Astrophysics 2009 Decadal Survey**

Moving From Science Objectives to Functional Requirements

Iterate As Necessary

Science Objectives

- Tied to NASA Priorities
- Offer major , not incremental, advances in the subject area
- Offer testable hypotheses
- Include a *baseline* and *performance Threshold* set, each with clear requirements

Measurement Requirements

- Quantitative requirements for each measurement
- Linked clearly to objectives and hypotheses
- Linked clearly to the *baseline* and *performance Threshold* science

Science Payload Requirements

- Quantitative performance requirements for each instrument (e.g., spectral range and resolution, spatial resolution, signal to noise, power, mass, etc.)

Spacecraft Requirements

- Quantitative requirements derived from payload and observational requirements (e.g., pointing, power, data handling, etc.)

Mission Requirements

- Where does the payload need to go?
- How long does it need to be there?
- What are the observing geometry requirements, lighting requirements, etc.?

Data Requirements

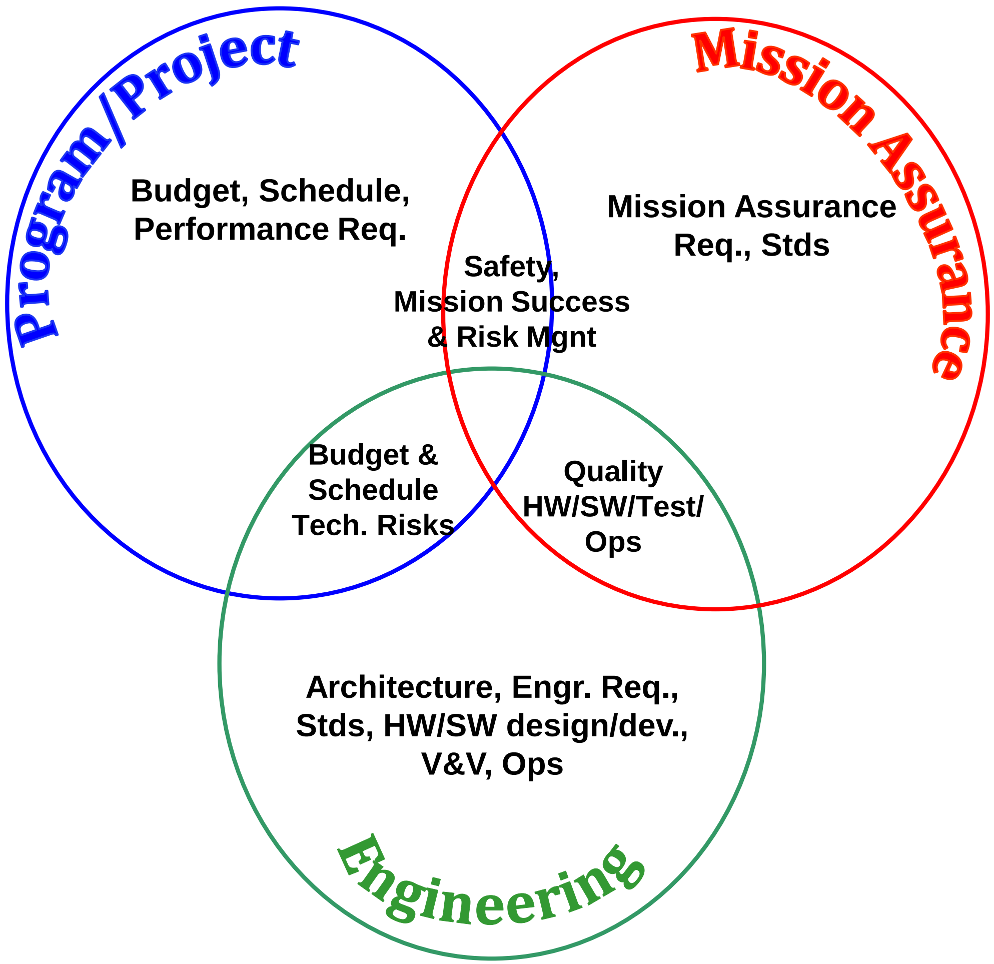
- Data volume for each investigation
- Algorithms to be used in analysis
- Schedule of data deliverables
- Data system functional requirements

This Has to Be Right!

Origins of the Engineering Technical Authority

- **ETA implementation is driven by:**
  - NASA's response to the Columbia Accident Investigation Board (CAIB) Report.
  - Administrator's objective to reestablish the highest level of engineering performance and quality across all of NASA as mandated in NPD 1000 and NPR 7120.5E
- **Examples of issues that ETA is intended to prevent:**
  - STS 1 saw foam impact on Columbia's wing, question was raised as to whether specification for tiles should be changed to include impact. Decision was no, based on cost and schedule.
  - Challenger 'O' ring is a case where, if the engineers had a direct line to a high level authority at NASA HQ, they at least could have been sure the technical issue was understood by the decision makers.
- **NASA's Strategic Management & Governance Handbook sets up a "Checks and Balances" organization model and authorizes "engineering to maintain technical purview over requirements and any deviations".**
- **The Project Systems Engineer is the project focal point for implementation of Engineering Technical Authority (ETA) at JPL.**

Context for Engineering Technical Authority



The objective of checks and balances is to expose issues/ problems early enough so that they can be resolved effectively.

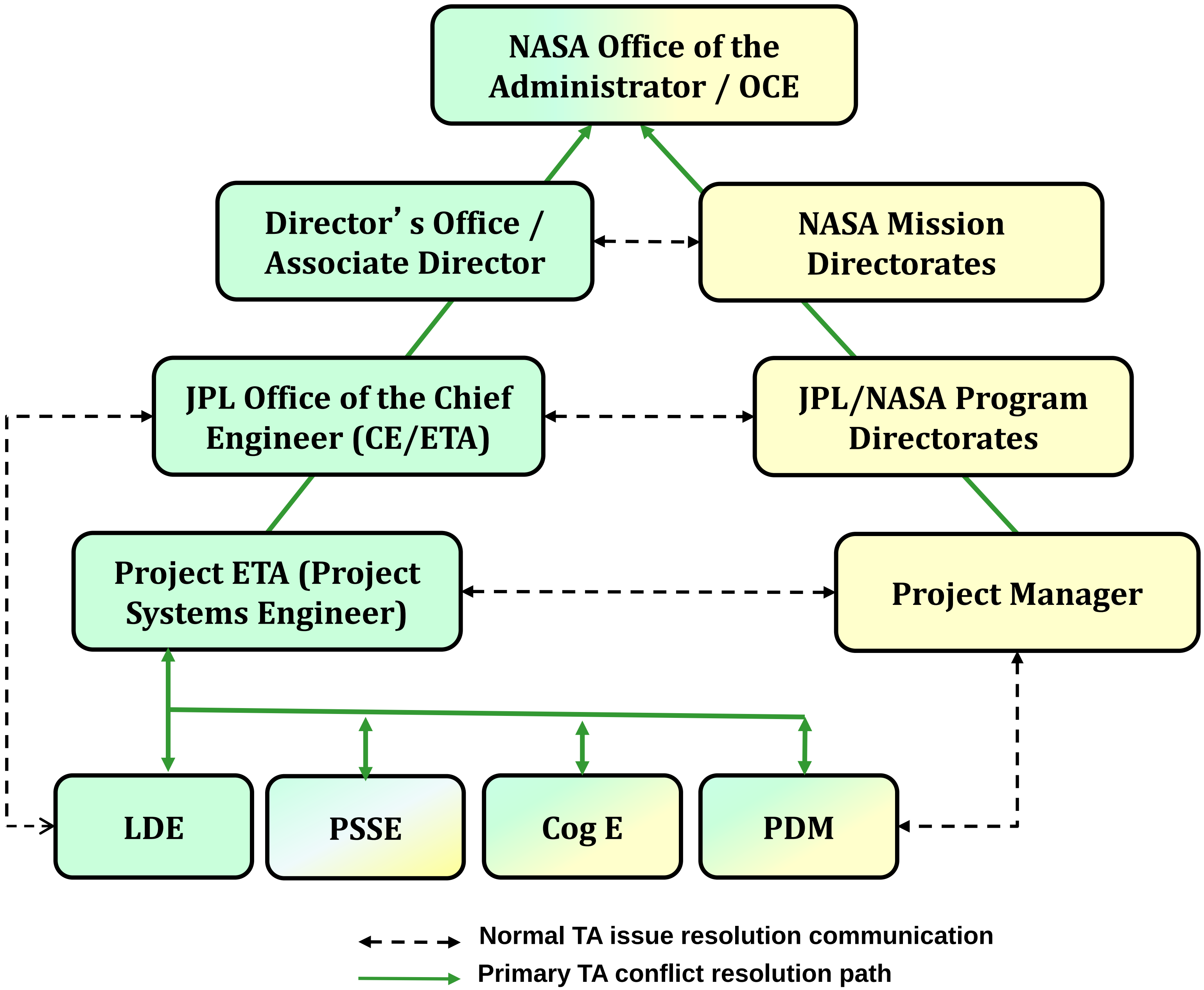
From NPD 1000.0: "Checks and Balances – NASA employs a system of checks and balances for effective internal control and to ensure the successful achievement of missions, assigning proper levels of influence and action to different organizations.

Program and project management focuses upon execution.

Engineering maintains independent authority by setting technical requirements, standards and approving any deviation from such requirements.

The Safety and Mission Assurance organization maintains responsibility for verification of programmatic compliance through strategies, policies and standards."

Hierarchy of ETA Issue Resolution Paths



PSE Responsibilities as the ETA

Project PSEs have the following additional responsibilities as Project ETAs:

- Own the technical requirements for the project .
- Establish compliance with or waive (working with OSMS and the JPL OCE), and implement all JPL institutional engineering requirements included in the Flight Project Practices and Design Principles.
- Report, on a regular basis request support as necessary for special problems or trade studies.
- Utilize NASA Engineering and Safety Center (NESC) as a technical resource for working detailed technical issues where independent expertise or review is needed. – For high technical risk requiring independent risk assessment,
- Verify that system-level FMECA, hazard analysis, PRAs, risk analyses, etc. are performed and results reported and incorporated into the overall engineering and risk assessment process.
- Attend and participate in major technical decision meetings with Center and NASA management
- At Safety and Mission S Reviews, provide risk assessment on all risks and be polled on readiness to proceed.
- Sign as the ETA on JPL's Certificate of Flight Readiness and Certificate of Critical Events Readiness.

Fault Protection

- **Every systems engineer is expected to be able to:**
  - Understand the off-nominal behavior of the systems they design, and
  - Know the benefits and limitations of fault protection as a way to understand and control off-nominal behavior
- **Every systems engineer is also expected to have some knowledge of:**
  - The basic principles and process steps used in the development, verification and validation, and operation of fault protection implementations

- **The set of missions historically flown by JPL has led to the development of robust autonomous FP capabilities**
- **FP capability fielded on Viking and Voyager, gradually increasing in scale to significant levels of complexity and autonomy**
- **MSL represents the most complex FP system JPL has built**
  - with 1097 system-level monitors and 38 system-level responses
  - plus on the order of 800 local responses

Characteristics of JPL FP Approach

- **Single-failure tolerance (SFT)**
  - No single point of failure will result in loss of mission
  - For some missions, waived in part or whole (e.g., single-string)

- **Limited use of reliability data**
  - JPL does not use reliability estimates as a basis for meeting single-failure tolerance requirements
  - Reliability estimates used for lifetime calculations
  - Reliability estimates used as supporting rationale in SFT waivers

- **Maintain failure tolerance after first failure**
  - Clear temporary failures
  - Maintain failure tolerance in safing modes
  - Robustness to multiple orthogonal failures

- **Fault protection as a systems engineering discipline**

Understanding Off-nominal Behavior

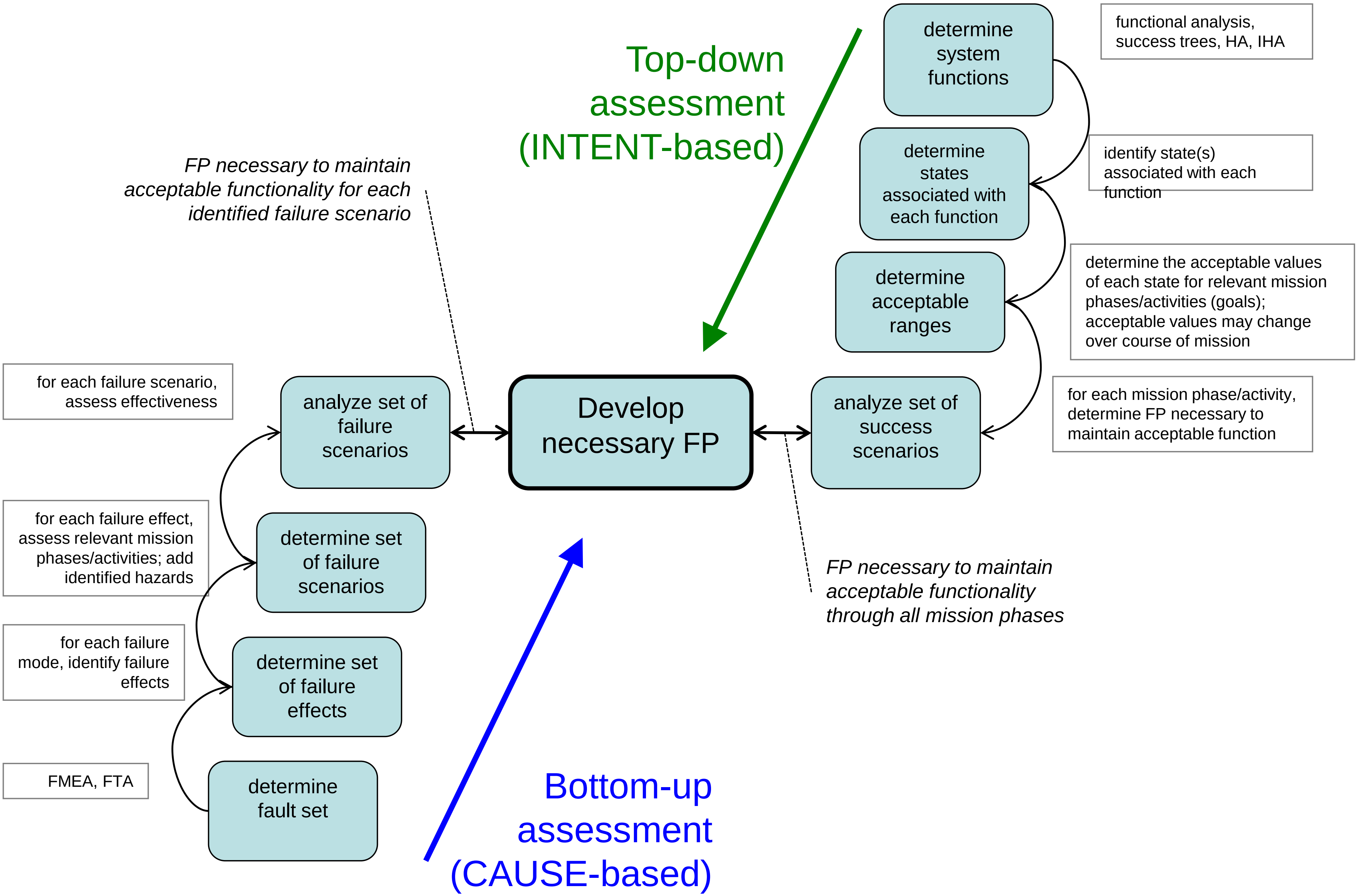
- **First off – What does "off-nominal mean"? What is NOMINAL behavior?**

- **Working Definition**
  – "Off-nominal is the class of behavior of a system that is unintended or unexpected"

- **What is "intent"?**
  – A description of what the system must do
  – Based on the need for which the system is being designed
  – A violation of intent is a **failure**

- **What is "expectation"?**
  – A description of the way the system is predicted to behave
  – Based on a model of the system
  – Different "observers" may have different expectations!
  – A violation of expectation is an **anomaly**

Top-Down and Bottom-up Analyses



A Strong V&V Culture

V&V is the process of confirming that the project's hardware, software, teams, and procedures are in compliance with functional, performance, environmental, design, and interface requirements, and that the aggregate is capable of satisfying mission objectives, level 1 requirements, and accomplishing operational scenarios.

- **Verification:** **Have we built the system right?**
  - Confirms compliance with **requirements**
  - Uses Test, Analysis, Inspection, Demonstration and combinations thereof
  - Test is the preferred method of V&V

- **Validation:** **Have we built the right system?**
  - Confirms that a verified end product fulfills its **intended use** when placed in its **intended environment**
  - Validation emphasizes end-to-end scenario testing, focuses on needed capabilities rather than requirements
  - Comes in **3 distinct flavors**:
    - **System Validation** – when people talk about "Validation" they generally mean this
    - Requirements Validation
    - Model Validation

V&V In the Project LifeCycle

Phase B (PRELIMINARY DESIGN)

Phase C (DESIGN & BUILD)

Phase D (ATLO)

Project Events and Test Activities:

- PMSR
- V&V Program Requirements
- PDR
- V&V Plan Development
- CDR
- Flight Integration & Unit/Subsystem/ Interface test & team training
- SIR
- ATLO Flight test/training
- EEIS/ORT RR
- Project V&V: Thread tests, EEIS, MST, ORT testing
- FRR

V&V Requirements and Plan Generation

Verification & Integration

System Validation

V&V Receivables:

- Project & Science Requirements
- Mission Plan (D)
- Ops Concepts (P)
- List s of interfaces (P)

- System requirements
- ISFD
- Lists of interfaces (F)
- Ops Concepts (F)
- Project Integration Plan (P)
- Mission System Fault Tree Mitigations (P)

- Mission Plan (F)
- System Requirements (F)
- Interfaces (SISs F; OIAs P)
- Ops Plan (P), Ops proc. List
- Training Plan (P)
- Project Integration Plan (F)
- Mission System Fault Tree mitigations (F)

- Delivered Testbed, Systems
- Ops Plan (F)
- Ops Procedures (P)
- Flight Rules (P)
- Dictionaries

- Delivered Flight/Ground Systems (P)
- Trained Teams

- Delivered Mission Systems (F)
- Flight Rules (F)
- Ops Proc (F)
- Interfaces (F)

V&V Deliverables:

- V&V Plan (D):
  - Verification Methods
  - Validation strategies
  - Roles & Responsibilities
  - Trace Matrix
- Testbed Functional Requirements

- V&V Plan (P):
  - Req. & I/F Ver.
  - Ops Concepts & critical event Validation
  - GS/FS I&T
  - ATLO/Testbeds
- Test Like You Fly Exceptions (P)

- V&V Plan (F):
  - Detailed Verification Program
  - Detailed Validation Program
  - Team & GDS, S/C Systems
  - Interfaces
- Incompressible Test List (P)
- Test Like You Fly Exceptions (F)
- Trace Matrices (P):
  - Requirements & I/Fs
  - Operations scenarios
  - Critical Inf. Flows

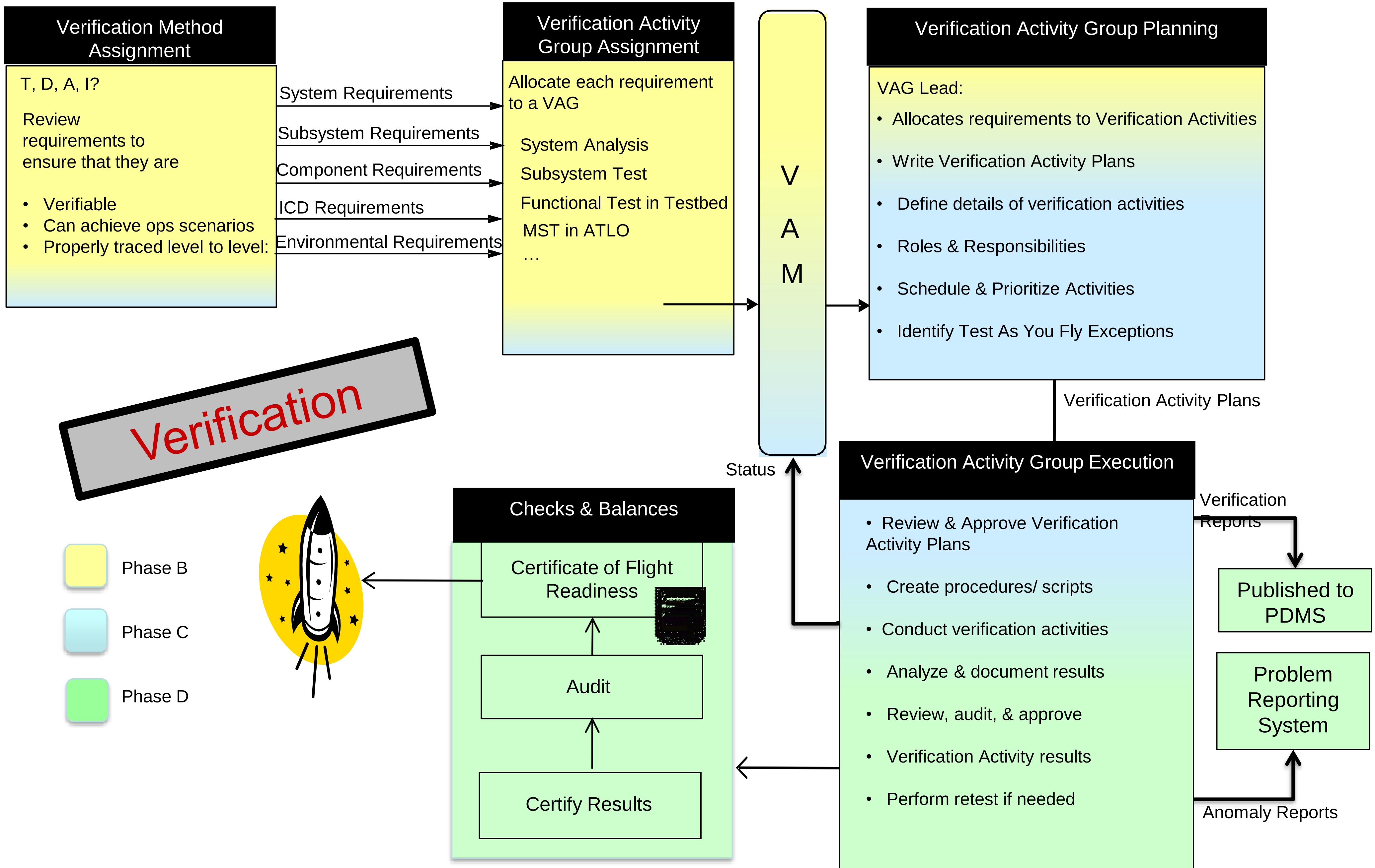
- V&V Activity Plans/Cases (F)
- Incompressible Test List (F)
- Test Like You Fly Exceptions List (U)
- Trace Matrices (Unpopulated) (F)

- Trace Matrices (populated)
- Test Cases:
  - Thread Tests
  - EEISTs
  - MSTs
  - ORTs
- Final Test Reports:
  - System Tests
  - Requirements & Interfaces
  - Training Certification

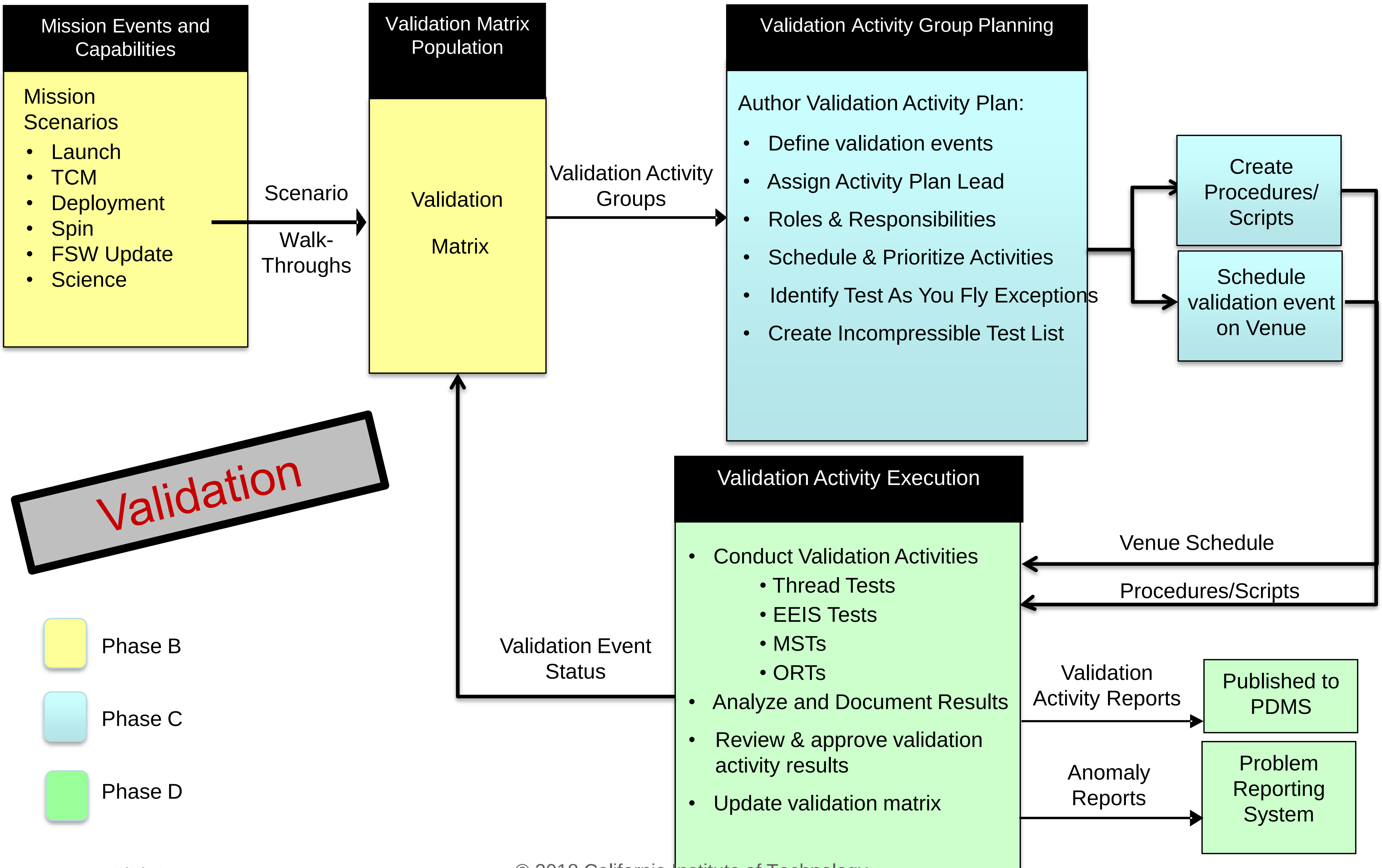
- Trace Matrices (populated)
- Final Test Reports:
  - Verification of Requirements & Interfaces
  - Validation Tests (Thread Test, EEIST, MST, ORT)

ATLO: Assembly Test & Launch Operations	GS: Ground System	PDR: Preliminary Design Review
CDR: Critical Design Review	I&T: Integration & Test	PMSR: Project Mgmt & System Req. Review
EEIS: End to End Information System	ISFD: Integrated Software Functional Diagram	RR: Readiness Review
FRR: Flight Readiness Review	MST: Mission Scenario Test	SIR: System Integration Review
FS: Flight System	ORT: Operations Readiness Test	V&V: Verification & Validation

Systems Verification



Systems Validation



The Incompressible Test List (ITL)

- **Purpose:** To identify critical tests that must be executed prior to launch. Keeps late-breaking descopes from eliminating critical tests.
  - Waivers must be written if ITL items are changed. This is not easy. Work hard to get your ITL items correct. (I.e. the ones that, if not completed you would quit the project before launching)
- ITL is delivered and signed at the SIR
  - Regular reporting expected between SIR and Launch
- Venue specification is essential for ITL testing
  - ATLO, testbed, Simulation environments are all valid ITL test platforms
- Note: The ITL should represent the true *minimum.* This doesn't define your entire V&V program. It just defines the minimum that you MUST do prior to Launch.
- Be specific enough that the scope can be understood by the team
  - (i.e., could you estimate how long that test would take?)
- Types of tests typically on ITL:
  - Verification of Flight System Design and Workmanship
    - Deployments, Phasing, Environments, Alignments, Hardware commands and telemetry, hardware integration /check-out procedures
  - Fidelity of System Testbed
    - Perform adequate tests to understand fidelity of flight system testbed(s)
  - Flight Software functionality esp. critical Fault Protection
  - Flight-like interfaces (DSN, UHF, etc.)
  - System level tests of mission-critical activities
  - Instrument and component specific calibrations

Example ITL

Table 4-1 Project Incompressible Test List

Incompressible Test List					
Item #	**name of test**	**Description**	**Test Article**	**Requirement Level**	**Pass Criteria**
ITL1	Instrument Comprehensive Performance Tests (CPT)	1. Pre-Environmental CPT1 2. Post Environmental CPT2 The intent of CPT2 is to verify performance remains unchanged post environmental test.	Instrument	L1, L2-PS, L3-Alg, L3-INS, L3-Cal	a, b, c, d, e, g
ITL2	RF Compatibility Tests	Ground Station and TDRS Compatibility Test verifies: RF and data format compatibility of uplink and downlink with Ground Stations, and TDRS including all telemetry and command data rates, all telecom configurations planned to be used during launch, and orbital ops phases.	Bus or Observatory	L2-PS, L3-SC, L3-MOS	a, b, c, g
ITL3	Solar Array Deployment and Flash Illumination Test	SA un-latch, full range motion and lock at end of travel (OSC only). Post delivery (OSC and VAFB) Flash Illumination test confirms electrical continuity throughout the EPS system and establishes baseline for future flash tests as needed.	Spacecraft System and Observatory	L3-SC	a, b, e, f

a. During test - Performs to the appropriate specifications of the hardware
b. During test - Provides proper data rate, throughput and output data, no significant data loss or corruption
c. During test -Valid telemetry, command, and sequences
d. Post test - Performs to the appropriate specifications of the hardware
e. Post test - No obvious damage or deterioration
f. Post test - Dimensionally stable or aligned correctly where no adjustment is required
g. Operates in all modes and conditions

7

"Test-As-You-Fly"

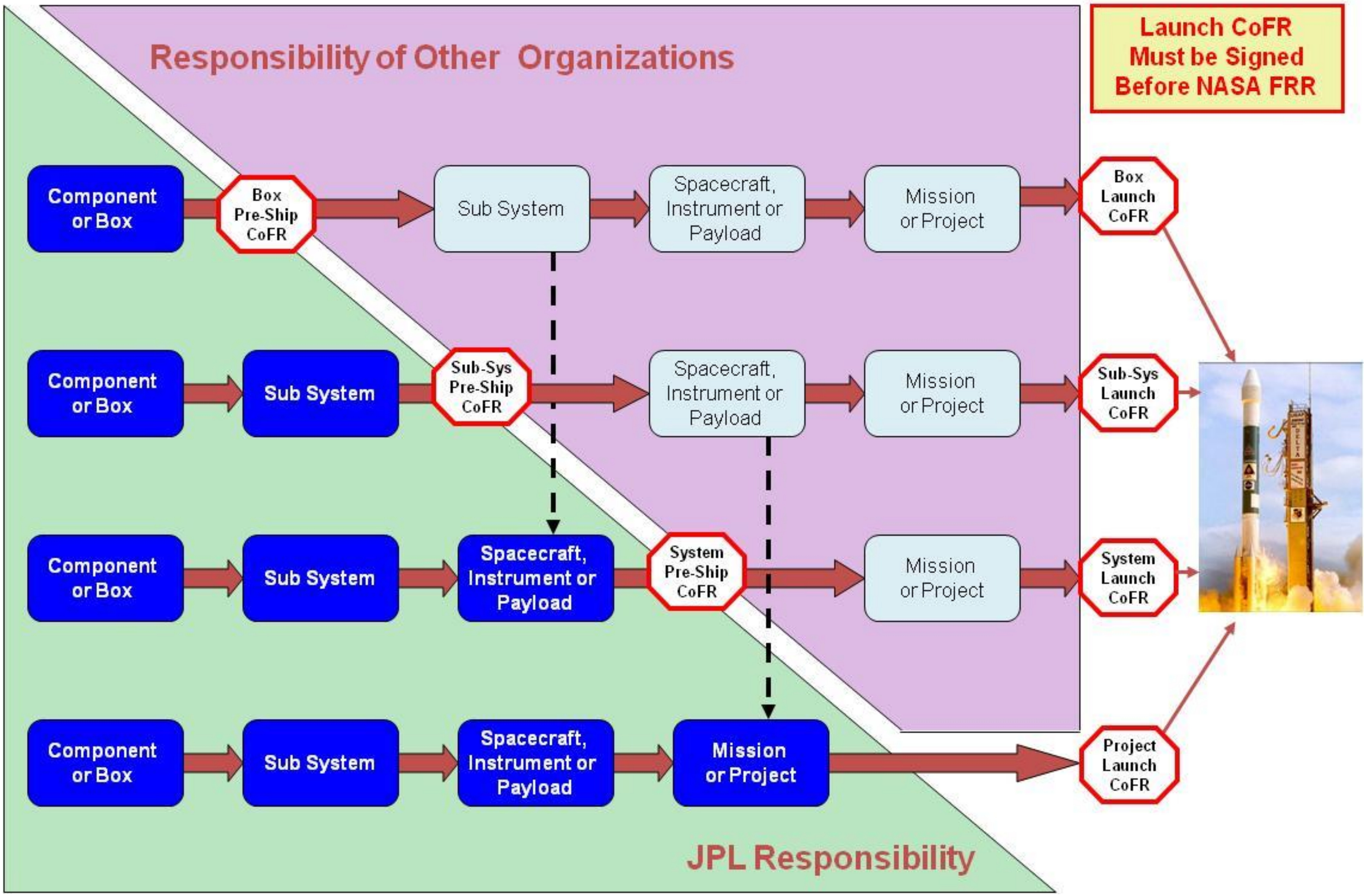
- **Test-As-You-Fly Principle**
  - Testing is performed as close as feasible to that to be encountered in flight
  - The Test-As-You-Fly Exceptions List *contains*
  - The deviations to the TAYF principle
  - The justification for the deviations (benefits and rationale)
  - The residual risk and mitigating actions
- **Reasons for "Test as you Fly" exceptions**
  - Facilities limitations
    - E.g., the T-Vac chamber is too small to allow solar array deployment
  - Earth-bound testing unable to duplicate in-space, on-orbit environment
    - E.g., weightlessness, solar radiation, magnetic fields, distances, etc.
  - Safety
    - E.g., propulsion system not fueled during tests
  - GSE limitations
    - E.g., Star tracker stimulus provides only static star fields

Certification of Flight Readiness

- **The formalization of the process for CoFR began in 2005**
- **Objective is to formally audit the processes (and products) that, when completed, constitute a flight ready system.**
  - Applies to all flight deliveries – assemblies, subsystems/Systems, Instruments or missions
  - Maximizes use of processes that we already do (minimal new work needs to be done)
- **Two areas are covered:**
  - Evidence of the project's adherence to JPL flight/mission development practices.
  - Tasks and products that document the project's residual risk to mission success.
- **The CoFR process is part of Project Life Cycle**
  - Organize libraries with CoFR processes in mind before formulation phase,- update continually
  - Use in reviews (PDR, CDR, ARR,etc.) to show work being done
  - Compliance verified by audit (OCE, SMA, AD) at earlier reviews
  - Start audit and signature process within the Project well before the pre-ship review and signed before NASA FRR

When is CoFR Required?

CoFR Requirement For JPL Projects



Certification of Flight Readiness (CoFR)

- JPL program and technical management certifies that sufficient due diligence has been adhered to for proceeding to flight.
  - They review compliance with institutional practices; DPs and FPPs, Incompressible Test List, review conduct, HRCRs/SRCRs.
  - They review compliance with engineering good practice; requirements, ICDs, V&V.
  - They review that you have a complete and released set of documents that evidence the above.
- This is conducted over multiple sessions nearer launch to allow time for document completion.
- This is done with spot checks to review quality of information, continuity in the process, and official release via signatures.
- They sign the CoFR when all of the artifacts and action items have been addressed.

Important CoFR Activities

- Define specifically and list what models and analysis archiving we will offer as evidence, i.e., CLA FEMs, reliability analysis, stress analysis
- Get feedback on the CoFR products list from Level 1-3 managers and system leads.
- Describe expectations in support of CoFR to Level 4-x, artifacts, CM, V&V.
- Define which documents are excluded from CoFR and requiring closure, i.e., non-functional requirements or test results documents like test plans and implementation plans.
- Define which WBS elements will have an HRCR.
- Define what specific documents will be provided for non-HRCRed elements.
- Define the V&V evidence approach will be used below Level 3.
- Recast project approach in the CoFR Template.
- Agree on CoFR artifacts and process with OCE.
- Establish with the JPL Office of the Chief Engineer (OCE) and signatories/stakeholders who will sign.

CoFR – Project Life Cycle Products

Project Life Cycle Products

	JPL Certification of Flight Readiness (page 2)									
	Project:									
	Completion of the following products document the project's adherence to JPL flight/mission system development practice. X's identify sign-off responsibility.	**SE**	**Sys Ctr**	**Lin Mgt**	**FSM/ MM**	**MAM**	**PM**	**OSMS**	**Remarks (attach additional documentation as needed)**	**Data Location (URL)**
1	System and subsystem design reviews, up to the MRR, including action item closures, are complete.	x	x	x	x	x	x			
2	System and subsystem environmental design and test requirements are documented, have been met and test reports released.	x	x	x	x	x	x	x		
3	System and subsystem design analyses (fault trees, FMECA, reliability, timing margin, functional models, mass properties, error budgets, etc.) are complete, been updated with test results, and reviewed.	x	x	x	x	x	x	x		
4	Hardware Drawings (ICD's, parts, assemblies, schematics, circuit data sheets, etc.) and design review documents, including action item closures, are released on under CM control.	x	x	x	x	x	x			
5	Software design description, source code, command and telemetry dictionary and design review documents, including action item closures, are released on under CM control.	x	x	x	x	x	x			
6	GDS, DSN and MOS design reviews (including mission design and navigation), through the ORR, including action item closures, are complete.	x	x	x	x	x	x			
7	HRCR, SRCR, inspection reports, log books, discrepancy reports, open analysis items, PFRs/ISAs (with audit by OSMS) and as-built list are complete and all open items closed out (and/or contractor approved equivalent	x	x	x	x	x	x	x		

CoFR – Residual Risks

Residual Risks

JPL Certification of Flight Readiness (page 3)

Project:

	Completion of the following tasks and products document the project's residual risk to mission success. X's identify sign-off responsibility.	SE	FSM/ MM	MAM	PM	OCE	ETA	OSMS	SM	Remarks (attach additional documentation as needed)	Data Location (URL)
8	Functional and performance requirements for complete and minimum mission success (including planetary protection) are documented and are being met.	x	x	x	x						
9	Institutional requirements compliance matrices, JPL Principles, Flight Project Practices have been audited and approved by OCE/OSMS.	x	x	x	x	x	x	x			
10	V&V requirements compliance matrix, including calibration, alignment and phasing tests and as run procedures and test/analysis reports complete and reviewed by OCE/OSMS.	x	x	x	x	x		x			
11	Testbed certification of equivalence to flight system complete and all differences documented and accounted for.	x	x	x	x						
12	Incompressible Test List (ITL) tests (including operational readiness tests with flight software and sequences) complete, reviewed and any deviations approved by the JPL Director	x	x	x	x	x		x	x		
13	Test as you fly exception list complete, reviewed by OCE/OSMS and approved by senior management.	x	x	x	x	x		x	x		
14	All safety compliance documents (e.g. MSPSP) have been approved.	x	x	x	x		x	x			
15	Commissioning activities, flight rules, launch/hold critieria, idiosyncracies, and contingency plans are complete, reviewed and delivered to the flight team.	x	x	x	x						
16	Waivers (with audit of mod/high risk and dissent by OSMS) and red flag PFRs (with audit by OSMS/OCE) are complete and approved.	x	x	x	x	x	x	x	x		
17	All external interface (e.g. DSN, L/V, foreign partners) design and operational issues have been closed.	x	x	x	x						
18	Flight hardware certified and any shortfalls for critical events readiness, to allow post launch development, has been identified, reviewed and approved by senior management.	x	x	x	x				x		
19	All post launch development work has been planned, reviewed and approved.	x	x	x	x				x		
20	All work-to-go to launch activities have been planned, reviewed and approved.	x	x	x	x			x	x		
21	Residual risk list complete, reviewed (including any dissents) and approved by senior management.	x	x	x	x	x		x	x		

Transition of SE Team to Operations

- You should plan to transition some set of development phase systems engineers to operations for some period of time.
  - Which SEs are transitioned and for how long depends a lot on the type of project and also the operations team and its philosophy
  - For shorter duration missions, it may be more efficient to transition much of the team as opposed to training an entirely new team.
  - For longer duration missions, the transition may be just through launch plus the initial critical activities.
  - Consider how important it is to carry the knowledge of the development team forward and in which areas.
- There will always be a conflict between development and operations workloads, regardless of whether you decide to transition SE folks to Ops or not.
  - Don't assume by not transitioning your SEs to Ops that they will not be distracted from the development workload with Ops type activities.
  - Work with the PM and the Mission Ops Manager to be sure the conflict is appropriately balanced and funded appropriately across WBS elements.

Behaviors of a JPL Systems Engineer

1. Has Intellectual Curiosity
2. Sees The “Big Picture” View
3. Sees Connections
4. Is Comfortable With Change
5. Is Comfortable With Uncertainty
6. Has “Proper Paranoia”
7. Keeps Track of Resources & Margins
8. Has Good Communication Skills
9. Has Self-Confidence and Energy
10. Has Appreciation For Process

Find The Fault!

Changing Environment

- **Challenges Facing JPL**
  - JPL and NASA busier than ever – personnel and facility resources stretched thin
  - Multiple strategic flagship missions in progress
  - Competed missions and instruments remain a priority
  - Increased number of Type2 (ClassD, smallsats, tech demo) missions
  - More partnerships (e.g. non-NASA sponsors, NASA Centers, industry, academia, international)
  - Continued generational demographic trends

- **What will these changes mean?**
  - Need for strong and experienced senior leaders with diverse set of skills
  - Even more emphasis on meeting project commitments despite constraints
  - Increased priority on following our proven "JPLWay" to mission success
  - Projects remain dependent on the line's technical expertise

National Aeronautics and Space Administration
Jet Propulsion Laboratory
California Institute of Technology
National Aeronautics and Space Administration

Model Based Systems Engineering at JPL

Where Do We Need to Improve our SE?

- Strengthen the quality of formulation products by allowing exploration of a more comprehensive option space and more rapid analysis of alternatives
- Perform early validation of system designs
- Give systems engineers time to do more engineering analysis and less paper management
- Significantly improve the quality of communications and understanding among system and subsystem engineers
- Achieve greater design reuse
- Align with the expectations and work habits of the next generation of engineering talent
  - this is the way new engineers are being trained and the way many of our early career engineers want to work

But the bottom line is to…

- **Reduce the number of product and mission defects in the face of growing complexity**
- **And increase productivity/reduce costs**

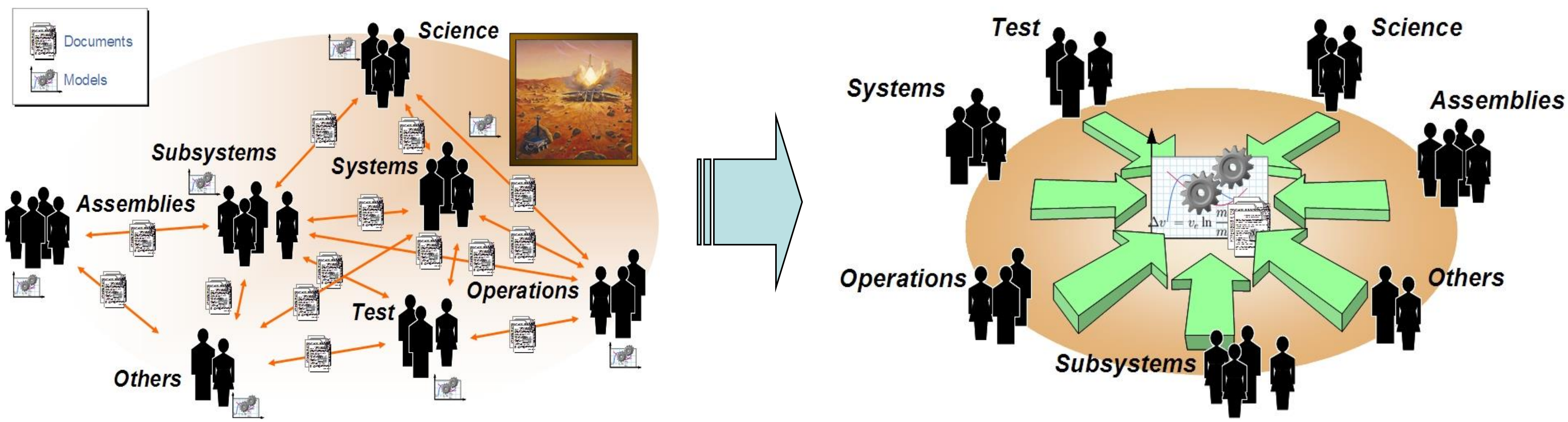
Integrated Model-Centric Engineering (IMCE)

- **IMCE is a JPL institutionally funded initiative established to support and accelerate the application of MBSE focuses on model-centric engineering practices. The scope and objectives for IMCE are:**
  - Developing an institutional re-usable MBSE capability
  - At all levels of system engineering discipline across the full system life cycle
  - Codifying MBSE practices and training our engineering workforce to apply MBSE for mission development
  - Helping project teams adopt and adapt institutional MBSE assets and practices

Vision and Mission

Vision: Transforming system engineering practices from silos and point-to-point connections to an integrated model-based practice

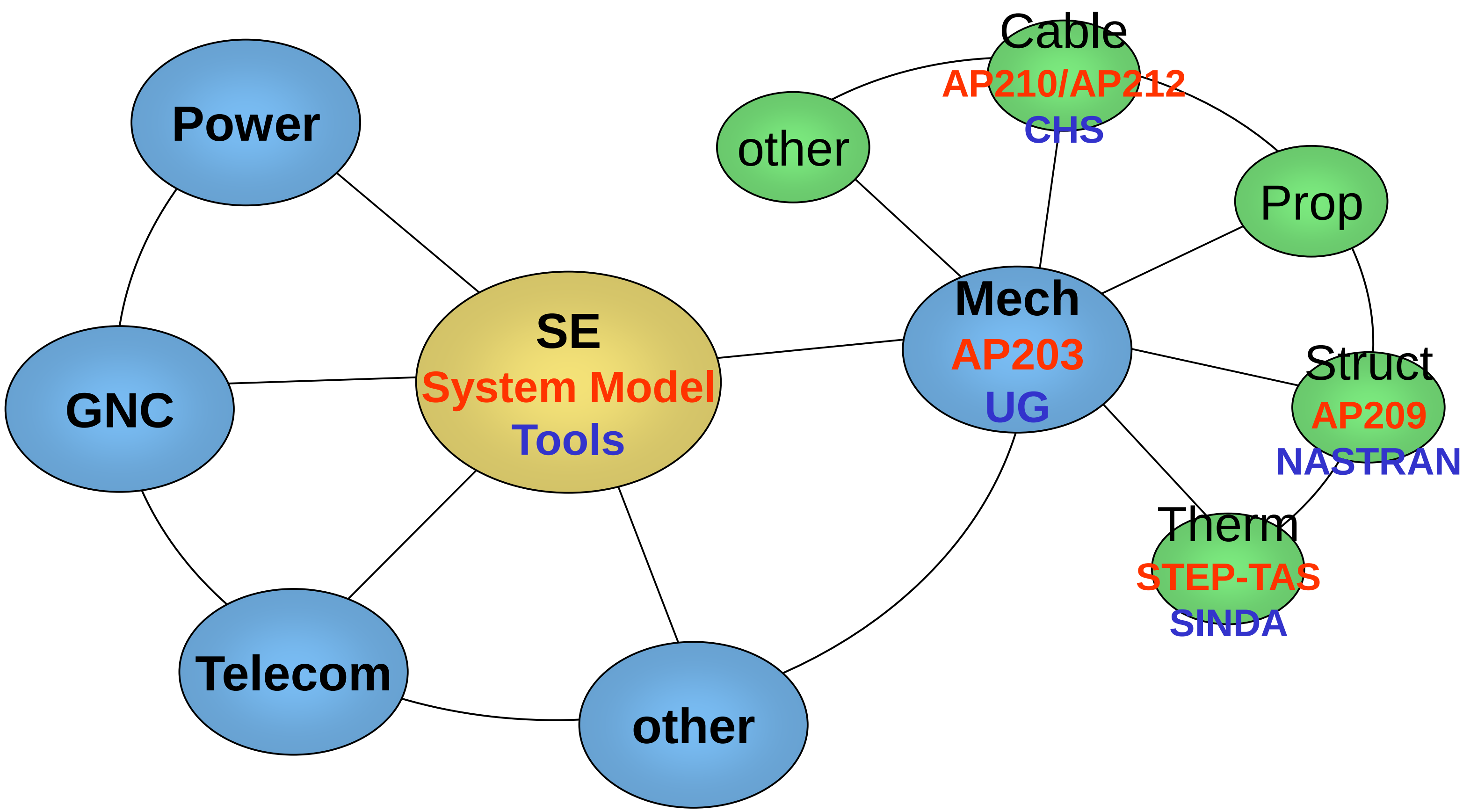
Mission: To facilitate the transformation from our current document-centric engineering practice to one in which structural, behavioral, physics and simulation-based models representing the technical designs are integrated and evolve throughout the life-cycle, supporting trade studies, design verification and system V&V



Today: Document driven & standalone models

Future: Reusable model-driven with integration & simulation capability

Concept of Integrated Model-Centric Engineering



The combination of ***Information Models***, ***Processes***, and ***Tools***

- enables simulation of system behavior, reasoning, long term data retentions and re-use
- information (e.g., requirements or mass) exist in a computer interpretable form and is associated with the simulation elements
- human interpretable documentation (i.e., a snapshot of system properties) can be automatically generated

IMCE Programmatic Development Approach

- It consists a multi-year roadmap for building institutional MBSE infrastructure and capabilities in three phases
- **Phase I: Initial MBSE Capability**
  - Establishing initial modeling infrastructure and developing MBSE workforce skills
- **Phase II: Maturing the Practice of MBSE**
  - Developing and capturing re-usable patterns and IP
  - Codifying model-based methodologies that cross formulation, flight systems, mission systems and key reviews
  - Expanding and integrating the tool set
- **Phase III: Integrating With Discipline-specific MBE**
  - Realizing fully integrated model-centric work practices and tools
  - The way we do work

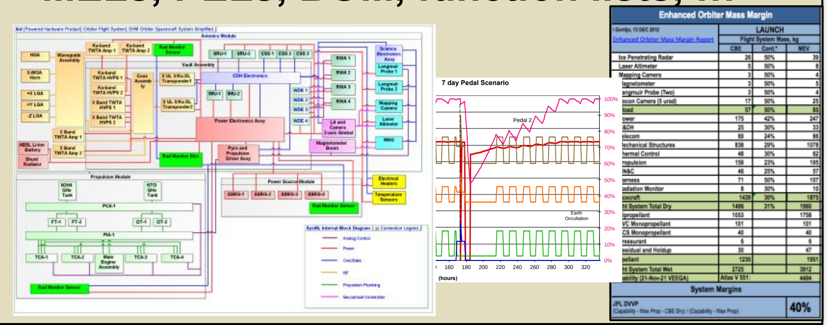
Technical Approach: Layered Architecture

Projects

Project Applications
(end users)

builds

- **Project products: block diagrams, MELs, PELs, BOM, function lists, …**



supplies

supplies

feedback

Discipline specialization and extensions from the IMCE Infrastructure

includes

IMCE

Discipline-specific MBSE capability: Owned by Doing Organization

- Specializations of core for electrical, mechanical, thermal, telecom, power, ..etc
- Codified processes and products (e.g, I-MEL. I-PEL)

model libraries	transforms	analyses/audits
SysML profiles/plugins/GUI		modeling patterns
systems engineering ontologies		

feedback

supplies

feedback

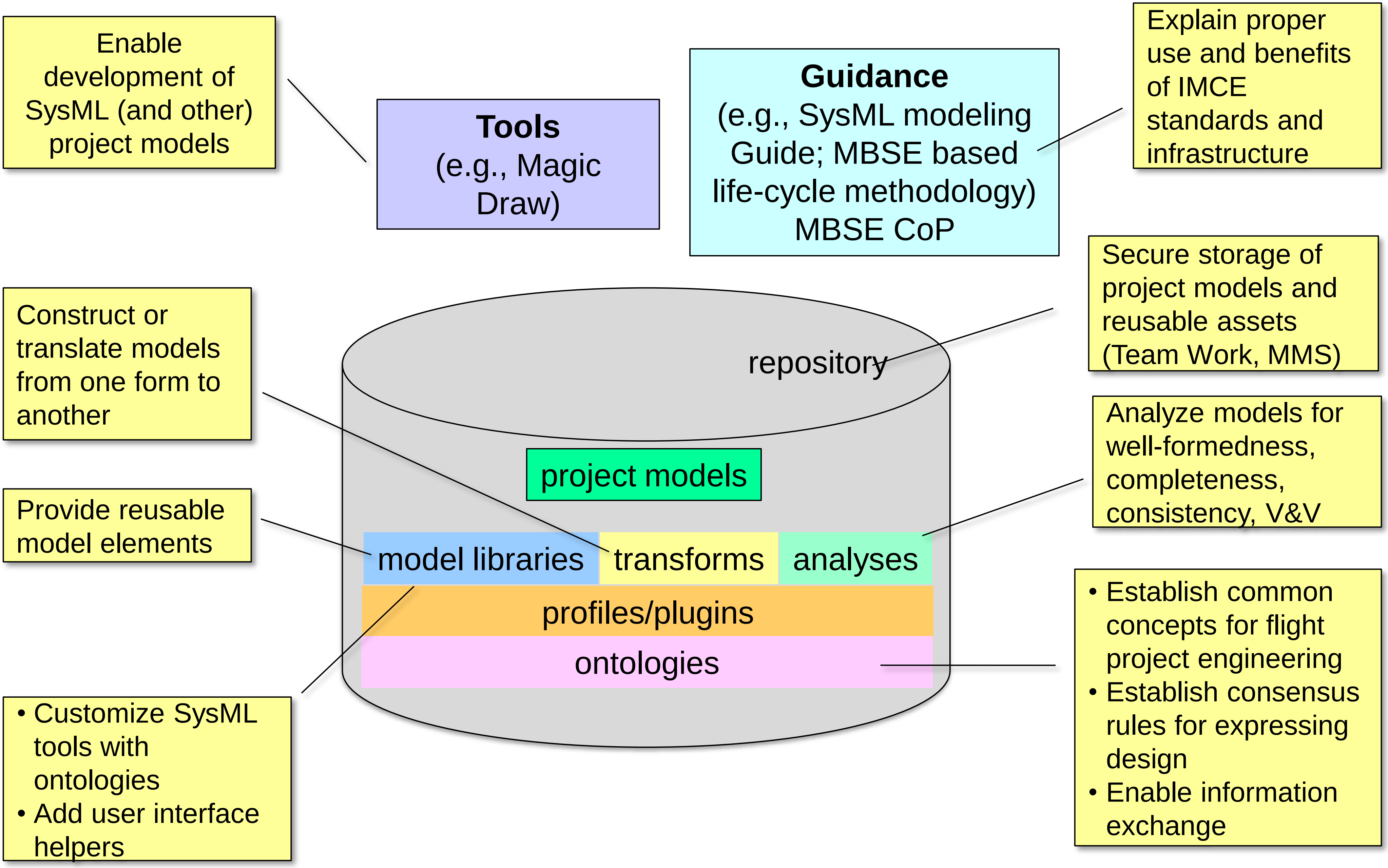
IMCE Infrastructure
(SE Standards)

includes

Core MBSE Capability: OMF compliant

model libraries	transforms	analyses/audits
SysML profiles/plugins/GUI		modeling patterns
systems engineering ontologies		

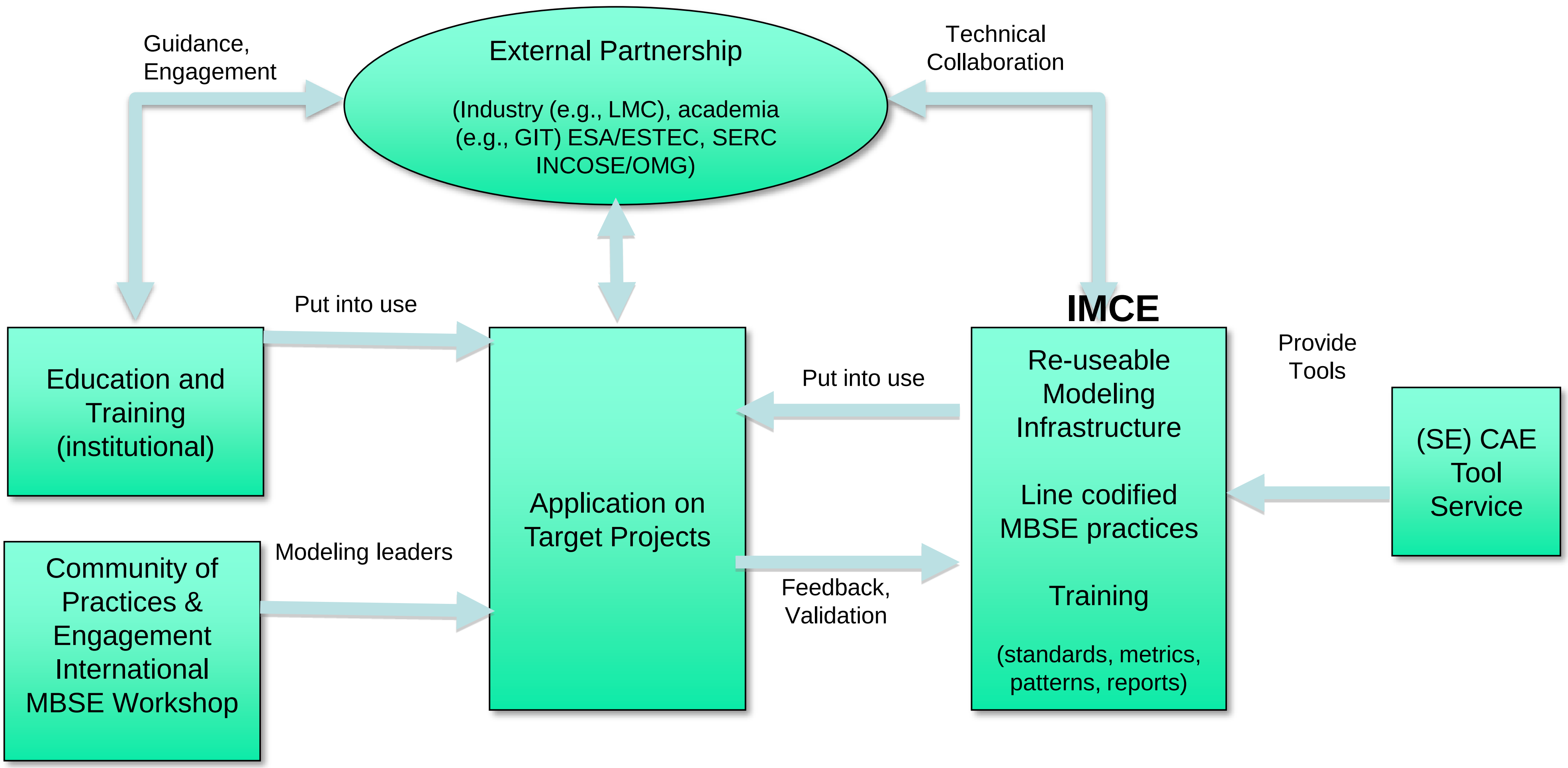
IMCE Core Infrastructure Elements



IMCE Infusion Approach

- **Conduct pilots to gain experience and know-how**
- **Look for project applications**
  - Europa Mission, Mars2020, AMMR, Psyche, etc
- **Team young engineers with senior SE practitioners**
- **Build MBSE community. E.G.,**
  - Organize and conduct workshops to share and stay current
  - Hold focus series discussion on project MBSE applications
- **Partner with other institutional key activities**
- **Partner with universities, industry and professional societies; e.g.,**
  - GIT, LM, INCOSE, OMG, SECR, ESA, AirBus
- **Codify know-how from experiences into formal repeatable methodologies, to be owned by line organization**

IMCE Ecosystem: Key MBSE Infusion Elements



MBSE Applications Realized

"Structural" Verification

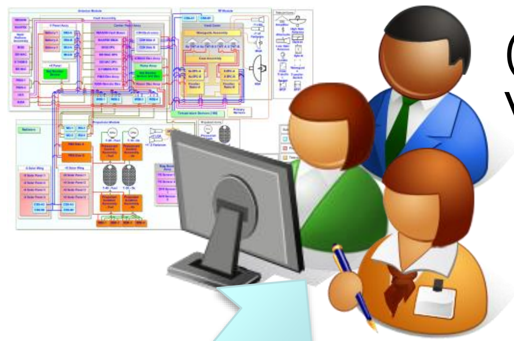
Results for Rule: hasConstrainedElement

Alert: CONSTRAINED ELEMENT: must have at least one constrained element
Description: Constraints that constrain anything other than ONE constrained element will FAIL this rule.
Applies To: ConstraintBlock
Total Elements Evaluated: 31

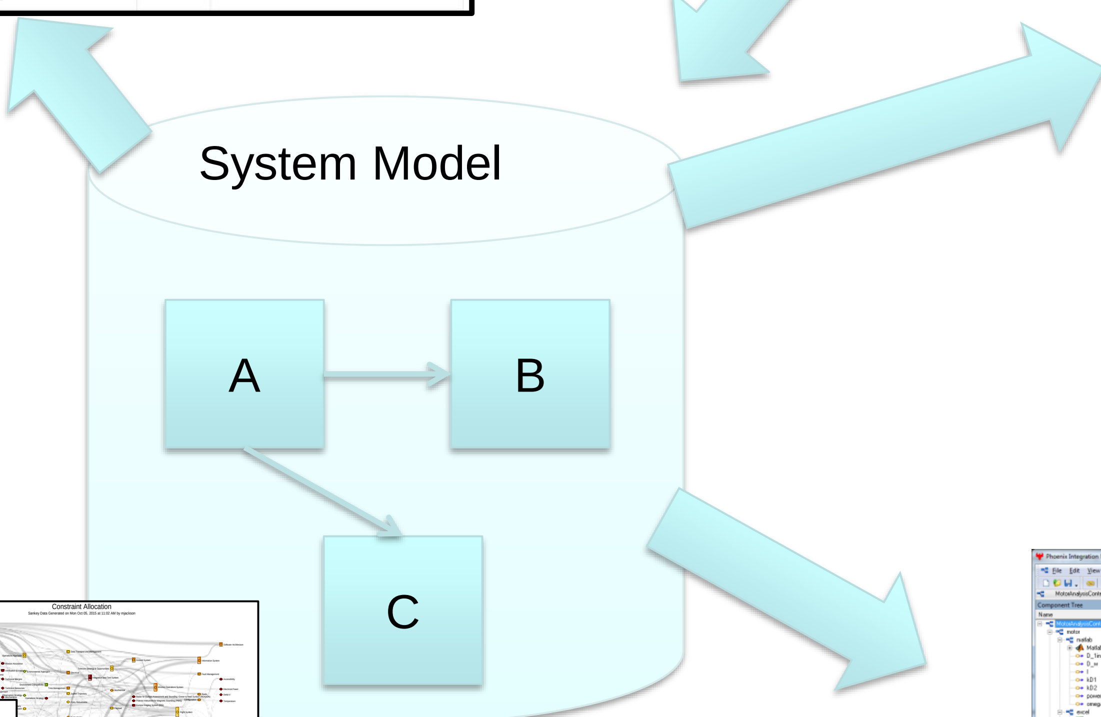
VIOLATORS: 14 | PASSED: 1 | SKIPPED: 0 | SKIPPED (N/A): 16 |

Afid	Name of Validated Element	Validation Result	Model ID
CT100.897	Duration Between Off-Sun Turns in Inner Cruise	FAILED	_Pt6XVOwvEeOA16G4SXuN9A
CT100.894	Temperature Limits during Faults in Adverse Environments	FAILED	_Pt8zmOwvEeOA16G4SXuN9A
CT100.900	Supplementary Heater Power on Off Hardware	FAILED	_Xb1FOuwvEeOA16G4SXuN9A
CT100.895	Temperature Limits during Faults with Abnormal Power Dissipations	FAILED	_Pt5JJOwvEeOA16G4SXuN9A

(Interactive) Views

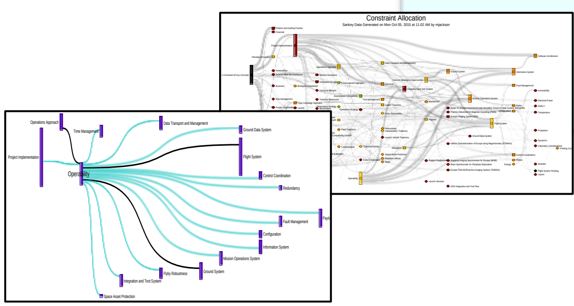


Gate Products

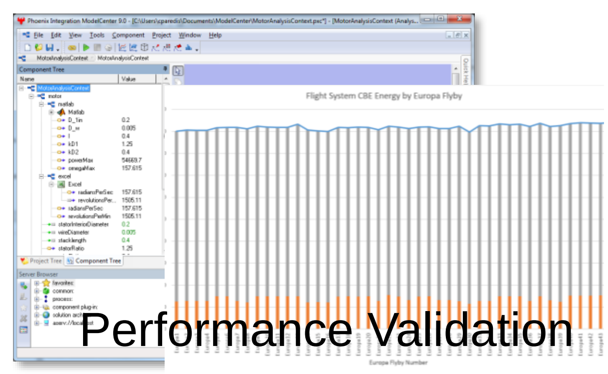


Repository

Custom visualizations



Performance Validation



Some Challenges

- **Modeling Environments – COTS tools, scalability, technology maturity, data exchange, visualization, user interface, value proposition**
- **Learning curve**
- **Paradigm shift /culture change**
  - It takes time
  - Can be disruptive
- **Change in workforce skills: modelers, team structure, infrastructure developers, software skills**
- **Model management, model-based review, model-based assurance**
- **Recognition of long term investment/resources needed to effect paradigm shift**
- **Etc.**

MBSE Value Proposition

- **MBSE uses modern information representation and modeling techniques to capture and link engineering data in such a way that:**
  - Consistency of the engineering data can be checked with the aid of computers
  - System performance analyses can be done in an integrated fashion
  - Information can be presented to stakeholders via **easily** customized views that are relevant to their specific interests
  - Data are stored in a single, integrated, authoritative source and updated throughout life-cycle
    - Waste lot of time in async processes and long email chains and can't find and end up redoing an analysis because we can't find it anymore
  - Contractual agreements (requirements) between systems and subsystems are expressed precisely and changes tracked rapidly
  - Flight/Ground trades via integrated mission operations simulations can be performed early

- **Overall, greater efficiency can be achieved in performing systems engineering functions as well as fewer "escapes'**

MBSE Infusion

- **Institution believes in ultimate value of MBSE**
- **Path to get there has not been easy and has been fraught with difficulty**
- **Very much a period of transition at JPL with different projects applying MBSE to very different degrees**
- **We are trying to figure out what works and are eager to gather information from the experiences of other organizations**

Differences Between Comparable Projects

- **Europa Clipper**
  - Mission design and elements are not new
  - But “concerns” are tightly coupled over a repetitive tour
- **2020**
  - Mostly a rebuild of an existing design
  - Focused around operability and contamination control
- **ARRM**
  - New operational modes
  - Multi center team
  - Technology demo on a large scale